CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Volume 10

Rolf H. Weber

DLT-Handelsplattformen

Spannungsfeld von Technologie und Recht

Mitarbeit: Okan Yildiz/Rainer Baisch

EIZ Publishing

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Schriften aus dem ITSL, herausgegeben von Florent Thouvenin und Rolf H. Weber

Volume 10

Rolf H. Weber

DLT-Handelsplattformen

Spannungsfeld von Technologie und Recht

Mitarbeit: Okan Yildiz/Rainer Baisch

EIZ Publishing

Verlag: EIZ Publishing (eizpublishing.ch)
Herausgeber: Center for Information Technology Society and Law ITSL, Florent Thouvenin (Hrsg.)
Produktion & Vertrieb: buch & netz (buchundnetz.com)
ISBN:
978-3-03805-535-8 (Print – Softcover)
978-3-03805-536-5 (PDF)
978-3-03805-537-2 (ePub)
DOI: https://doi.org/10.36862/eiz-535
Version: 1.01 – 20221027

Dieses Werk ist als gedrucktes Buch sowie als E-Book (open access) in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: https://eizpublishing.ch/publikationen/dlt-handelsplattformen/.

Vorwort

Die Digitalisierung ist ein zentraler Faktor der Innovation und der Anpassung von Geschäftsmodellen in der Volkswirtschaft. Ein erster technologischer Schub ist vor dreissig Jahren mit der Einführung des Internet erfolgt. Die Distributed Ledger Technologie (DLT) hat in den letzten Jahren erneut zu stark veränderten Infrastrukturen im digitalen Bereich geführt. Diese neuen Technologien tragen sowohl im Finanzsektor als auch in anderen Wirtschaftsbereichen zu einem erheblichen, wenn zwar noch nicht abschliessend abschätzbaren Innovations- und Effizienzsteigerungspotential bei.

Der Gesetzgeber hat mit Anpassungen der regulatorischen Rahmenbedingungen relativ schnell reagiert (z.B. bei den Bankregulierungen und durch den Erlass des DLT-Gesetzes mit der Schaffung von Registerwertrechten und DLT-Handelsplattformen). Im Grundsatz beabsichtigen Politik und Recht, für optimale Rahmenbedingungen zu sorgen, damit die neuen Technologien den Bedürfnissen der Gesellschaft und der Märkte gerecht zu werden vermögen; im Finanzmarktbereich gilt für die Schweiz ein prinzipienbasierter sowie technologie- und wettbewerbsneutraler Regulierungsansatz. Im Besonderen hat zusätzlich zu den seit anfangs 2016 durch das FinfraG geschaffenen neuen Formen von Handelsplattformen das DLT-Gesetz die Einrichtung von DLT-Handelssystemen ermöglicht; der gleichzeitige Austausch von Angeboten unter mehreren (auch privaten) Teilnehmenden sowie der Vertragsabschluss nach nicht diskretionären Regeln erlauben den multilateralen Handel mit DLT-Effekten.

Die Thematik der DLT-Handelsplattformen ist technologisch und rechtlich weiterhin stark im Fluss. Eine vertiefte Auslotung des normativen Regulierungsrahmens erweist sich deshalb als angebracht. Der Autor hat sich bereits mehrfach mit kürzeren Beiträgen zu umstrittenen Rechtsfragen geäussert; die vorliegende Publikation soll die Gedanken in einem Gesamtüberblick zusammenführen. Besonderer Dank für die wertvolle Unterstützung bei der Ausarbeitung der Publikation gebührt MLaw Okan Yildiz und MLaw & Dipl. Kaufm. univ. Rainer Baisch; weiter zu danken ist der SIX Exchange AG für den Finanzierungsbeitrag zur Erstellung dieser Studie. Die Ausführungen sind auf dem Stand von September 2022; die Angaben auf weiterführende Dokumente sind verlinkt; Hinweise nimmt der Autor gerne entgegen.

Zürich, im September 2022 Rolf H. Weber

Inhaltsverzeichnis

Literaturverzeichnis

Alle Internet-Dokumente sind letztmals am 7. September 2022 besucht worden.

A

Aggarwal/Kumar, 2021. Shubhani Aggarwal/Neeraj Kumar, Attacks on blockchain. In: Shubhani Aggarwal/Neeraj Kumar/Pethuru Raj (eds.), The Blockchain Technology for Secure and Smart Applications across Industry Verticals, Advances in Computers, Cambridge MA 2021, 399–410

Akbar/Muneer/ElHakim/Fati, 2021. Nur Arifin Akbar/Amgad Muneer/Narmine ElHakim/Suliman Mohamed Fati, Distributed Hybrid Double Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses, Future Internet 2021, No. 11:285, 1–20

Alexander, 2012. Kern Alexander, Market Structures, Technology and European Securities Regulation. In: Brigitte Strebel-Aerni (Hrsg.), Finanzmärkte im Banne von Big Data, Zürich 2012, 33-44

Ali, 2013. Shahla F. Ali, Consumer Financial Dispute Resolution in a Comparative Context: Principles, Systems and Practice, Cambridge 2013

Ali/Huang, 2012. Shahla F. Ali/Hui Huang, Financial Dispute Resolution in China: Arbitration or Court Litigation?, Arbitr. Int. 2012, 77–100

Allen/Lane/Poblet, 2019. Darcy W. E. Allen/Aaron M. Lane/Marta Poblet, The Governance of Blockchain Dispute Resolution, Harv. Negot. Law Rev. 2019, 75–101

Andreotti, 2023. Fabio Andreotti, Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht. Eine Analyse unter Erarbeitung eines Rechtsprinzips der Dezentralität, Diss. Zürich 2023 (nicht verarbeitet, erscheint anfangs 2023)

Antonopoulos, 2017a. Andreas M. Antonopoulos, Mastering Bitcoin, Programming the Open Blockchain, 2nd ed. Beijing 2017

Antonopoulos, 2017b. Andreas M. Antonopoulos, Mastering Bitcoin, Unlock Digital Cryptocurrencies, Sebastopol 2017

Antonopoulos/Wood, 2019. Andreas M. Antonopoulos/Gavin Wood, Mastering Ethereum, Building Smart Contracts and DApps, Beijing 2019

Arifeen et al., 2021. Md. Murshedul Arifeen/Abdullah Al Mamun/Tanvir Ahmed/M. Shamim Kaiser/Mufti Mahmud, A Blockchain-Based Scheme for Sybil Attack Detection in Underwater Wireless Sensor Networks. In: M. Shamim Kaiser/Anirban Bandyopadhyay/Mufti Mahmud/Kanad Ray (eds.), Proceedings of TCCE 2020, Singapore 2021, 467–476

Ast/Deffains, 2021. Federico Ast/Bruno Deffains, When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice, Stanford JBLP 2021, 241–257

B

Baird/Harmon/Madsen, 2020. Leemon Baird/Mance Harmon/Paul Madsen, Hedera Hashgraph Whitepaper, Hedera: A Public Hashgraph Network & Governing Council – The trust layer of the internet, last updated August 2020, aufrufbar unter <https://hedera.com/hh_whitepaper_v2.1-20200815.pdf>

Baisch/Baumann/Weber, 2014. Rainer Baisch/Simone Baumann/Rolf H. Weber, «Shades of grey» in Dark Pools, GesKR 2014, 183-198

Baisch/Weber, 2021. Rainer Baisch/Rolf H. Weber, Entwicklungen im europäischen Finanzmarktrecht – «Digital Finance Package», «Brexit means Brexit», und Corona-Reaktionen. In: Astrid Epiney/Petru Emanuel Zlatescu (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2020/2021, Zürich 2021, 221-242

Baisch/Weber, 2022. Rainer Baisch/Rolf H. Weber, Entwicklungen im europäischen Finanzmarktrecht – «Sustainable Finance» und DLT-Regulierung. In: Astrid Epiney/Petru Emanuel Zlatescu (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2021/2022, Zürich 2022, 173–193

Baker/Werbach, 2019. Colleen Baker/Kevin Werbach, Blockchain in Financial Services. In: Jelena Madir (ed.), FinTech, Law and Regulation, Cheltenham/Northampton 2019, 123–147

BeckOK BGB-*Bearbeiter/in*. Wolfgang Hau/Roman Poseck (Hrsg.), Beck'scher Online-Kommentare, BeckOK BGB, 57. Edition, München 2021

Bieri/Powell, 2021. Adrian Bieri/Julian Powell, Meldung von Verletzungen der Datensicherheit, AJP 2021, 780–787

Bissell/Lasalle/Dal Cin, 2019. Kelly Bissell/Ryan M. Lasalle/Paolo Dal Cin, The Cost of Cybercrime, Ninth Annual Cost Of Cybercrime Study, Unlocking The Value Of Improved Cybersecurity Protection, North Traverse City 2019, aufrufbar unter <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom%3d50>

Bissias/Ozisik/Levine/Liberatore, 2014. George Bissias/A. Pinar Ozisik/Brian N. Levine/Marc Liberatore, Sybil-Resistant Mixing for Bitcoin, WPES '14: Proceedings of the 13th Workshop on Privacy in the Electronic Society 2014, 149–158

BK OR-*Fellmann*. Walter Fellmann, Berner Kommentar, Band VI: Obligationenrecht. 2. Abteilung: Die einzelnen Vertragsverhältnisse. 4. Teilband: Der einfache Auftrag, Art. 394-406 OR, Bern 1992

BSK BV-*Bearbeiter/in*. Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015

BSK FinfraG-*Bearbeiter/in*. Rolf Watter/Rashid Bahar (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz, Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019

BSK IPRG-*Bearbeiter/in*. Pascal Grolimund/ Leander D. Loacker/Anton K. Schnyder (Hrsg.), Basler Kommentar zum Internationalen Privatrecht, 4. Aufl., Basel 2020

BSK OR-*Bearbeiter/in*. Corinne Widmer Lüchinger/David Oser (Hrsg.), Basler Kommentar, Obligationenrecht I, 7. Aufl., Basel 2020

Buchwald, 2020. Michael Buchwald, Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration, Univ. Pa. Law Rev. 2020, 1369–1423

C

Cai/Fragkos/Tsiropoulou/Veneris, 2020. Yuxi Cai/Georgios Fragkos/Eirini Eleni Tsiropoulou/Andreas Veneris, A Truth-Inducing Sybil Resistant Decentralized Blockchain Oracle, 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services 2020, 128–135

Caldarelli, 2020. Giulio Caldarelli, Understanding the Blockchain Oracle Problem: A Call for Action, Information 2020, 1–19

Calliess/Baumgarten, 2020. Christian Calliess/Ansgar Baumgarten, Cybersecurity in the EU, The Example of the Financial Sector: A Legal Perspective, GLJ 2020, 1149–1179

Camillo, 2017. Mark Camillo, Cybersecurity: Risks and management of risks for global banks and financial institutions, J. Risk Manag. Financ. Inst. 2017, 196–200

Carbonara/Guerra/Parisi, 2016. Emanuela Carbonara/Alice Guerra/Francesco Parisi, Sharing Residial Liability: «Cheapest Cost Avoider» revisited, J. Leg. Stud. 2016, 173–201

Chentouf/Bouchkaren, 2021. Fatima Zahrae Chentouf/Said Bouchkaren, Blockchain for Cybersecurity in IoT. In: Yassine Maleh/Youssef Baddi/Mamoun Alazab/Loai Tawalbeh/Imed Romdhani (eds.), Artificial Intelligence and Blockchain for Future Cybersecurity Applications, Cham 2021, 61–84

Chevalier, 2021. Maxime Chevalier, From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order, J. Int. Dispute Settl. 2021, 558–584

Chevallier, 1996. Jacques Chevallier, Les lois expérimentales. In: Danièle Bourcier/Claude Thomasset (éds), L'écriture du droit … face aux technologies et l'information, Paris/New York/Amsterdam 1996, 167–203

Chohan, 2021. Usman W. Chohan, Non-Fungible Tokens: Blockchain, Scarcity, and Value, Critical Blockchain Research Initiative, 24th March 2021

Contratto, 2014. Franca Contratto, Hochfrequenzhandel und systemische Risiken, GesKR 2014, 143-160

Cornelius, 2002. Kai Cornelius, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353–358

Curran, 2018. Brian Curran, What are Oracles? Smart Contracts, Chainlink & «The Oracle Problem», last updated September 2018, aufrufbar unter <https://blockonomi.com/oracles-guide/>

D

Das/Faust/Loss, 2019. Poulami Das/Sebastian Faust/Julian Loss, A Formal Treatment of Deterministic Wallets, CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London 2019, 651–668

de Miranda, 2019. Patricia L. de Miranda, Cybersecurity and Blockchain. In: Jelena Madir (ed.), FinTech, Law and Regulation, Cheltenham/Northampton 2019, 208–231

Del Duca/Rule/Rimpfel, 2014. Louis F. Del Duca/Colin Rule/Kathryn Rimpfel, eBay's De Facto Low Value High Volume Resolution Process: Lessons and Best Practices for ODR Systems Designers, ALR 2014, 204–219

Deng/Lee, 2017. Robert Deng/David Kuo Chuen Lee, Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 2, Cambridge MA 2017

Diehl, 2021. Martin Diehl, Formen programmierbaren Geldes und Rolle der Zentralbank. In: Sebastian Omlor/Mathias Link (Hrsg.), Kryptowährungen und Token, Frankfurt am Main 2021, 43–71

Douceur, 2002. John R. Douceur, The Sybil Attack. In: Peter Druschel/Frans Kaashoek/Antony Rowstron (Hrsg.), Peer-to-Peer Systems, Berlin/Heidelberg/New York 2002, 251–260

Drescher, 2017. Daniel Drescher, Blockchain Grundlagen, Frechen 2017

E

Eggen, 2011. Mirjam Eggen, Finanzprodukte – Auftrag oder Kauf?, SZW 2011, 625–638

Eggen, 2018. Mirjam Eggen, Smart Contracts und allgemeine Geschäftsbedingungen. In: Susan Emmenegger/Stephanie Hrubesch-Millauer/Frédéric Krauskopf/Stephan Wolf (Hrsg.), Festschrift für Thomas Koller, Bern 2018, 155–175

Eggen, 2021. Mirjam Eggen, Vertragsfreiheit in der Wolke, AJP 2021, 577–592

Eggen/Sillaber, 2020. Mirjam Eggen/Christian Sillaber, DLT-Handelssysteme. In: Jusletter 11. Mai 2020

Eggen/Stengel, 2020. Mirjam Eggen/Cornelia Stengel, Optionen zur rechtlichen Ausgestaltung von digitalem Zentralbankgeld (Wholesale CBCD), GesKR 2020, 200–214

English/Kim/Nonaka, 2018. Erin English/Amy Davine Kim/Michael Nonaka, Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry, Microsoft Publications 2018

Eskandari/Barrera/Stobert/Clark, 2018. Shayan Eskandari/David Barrera/Elizabeth Stobert/Jeremy Clark, A First Look at the Usability of Bitcoin Key Management, arXiv:1802.04351 (2018), 1–10

F

Favrod-Coune/Belet, 2018. Pascal Favrod-Coune/Kévin Belet, La convention d'arbitrage dans un smart contract, PJA 2018, 1105–1117

Fischer/Schneuwly, 2021. Jonas Fischer/Anne Mirjam Schneuwly, Alternative Dispute Resolution – Verhandlung, Mediation, Schlichtung, Schiedsgerichtsbarkeit, Schiedsgutachten, Hybride ADR-Verfahren, Zürich/St. Gallen 2021

Furrer, 2018. Andreas Furrer, Die Einbettung von Smart Contracts in das schweizerische Privatrecht, Anwaltsrevue 2018, 103–115

G

Ganne, 2018. Emmanuelle Ganne, Can Blockchain revolutionize international trade?, Geneva 2018

Ganne, 2021. Emmanuelle Ganne, Blockchain's Practical and Legal Implications for Global Trade and Global Trade Law. In: Mira Burri (ed.), Big Data and Global Trade Law, Cambridge 2021, 128–159

Gauch/Schluep/Emmenegger, 2020. Peter Gauch/Walter R. Schluep/Susan Emmenegger, OR AT, Schweizerisches Obligationenrecht, Allgemeiner Teil, Band II, 11. Aufl., Zürich 2020

Gervais et al., 2016. Arthur Gervais/Ghassan O. Karame/Karl Wüst/Vasileios Glykantzis/Hubert Ritzdorf/Srdjan Capkun, On the Security and Performance of Proof of Work Blockchains, CCS '16: Proceedings of the 2016 ACM SIGSAC, Vienna 2016, 3–16

Girsberger/Peter, 2019. Daniel Girsberger/James Thomas Peter, Aussergerichtliche Konfliktlösung, Kommunikation – Konfliktmanagement – Verhandlung – Mediation – Schiedsgerichtsbarkeit, Zürich/Basel/Genf 2019

Girsberger/Voser, 2021. Daniel Girsberger/Nathalie Voser, International Arbitration, Comparative and Swiss Perspectives, 4. Aufl., Zürich/Basel/Genf 2021

Glatz, 2018. Florian Glatz, Blockchain. In: Stephan Breidenbach/Florian Glatz (Hrsg.), Rechtshandbuch Legal Tech, München 2018, 59–90

Göbel/Keeler/Krzesinski/Taylor, 2016. Johannes Göbel/H. Paul Keeler/Anthony Krzesinski/Peter Taylor, Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay, Perform. Evaluation 2016, 23–41

Guillaume, 2019. Florence Guillaume, Aspects of private international law related to blockchain transactions. In: Daniel Kraus/Thierry Obrist/Olivier Hari (Hrsg.), Blockchains, Smart Contracts, Decentralised Autonomous Organizations and the Law, Cheltenham/Northampton 2019, 49–82

Guillaume/Riva, 2022. Florence Guillaume/Sven Riva, Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice. In: Andrea Bonomi/Matthias Lehmann (eds.), Blockchain and Private International Law, Leuven 2022, im Erscheinen, Draft aufrufbar unter <http://dx.doi.org/10.2139/ssrn.4042704>

Gut, 2014. Susanna Gut, Schiedsgerichtsbarkeit: eine Streitbeilegungsmethode für Anlegerstreitigkeiten, Diss. Zürich 2014

Gyr, 2019. Eleonor Gyr, Blockchain und Smart Contracts, Die vertragsrechtlichen Implikationen einer neuen Technologie, Diss. Bern 2019

H

Hagen, 2020. Julia Hagen, Regulatory Sandboxes – Ein Instrument für digitale Innovationen im Gesundheitssektor. In: Marco A. Pfannstiel/Kristin Kassel/Christoph Rasche (Hrsg.), Innovationen und Innovationsmanagement im Gesundheitswesen, Wiesbaden 2020, 163–179

Harasgama/Kleiner/Berger, 2022. Rehana Harasgama/Jan Kleiner/Viviane Berger, Cyberangriffe beim Bund, S&R 2022, 40–49

Hays et al., 2021. Demelza Hays/Katharina Gehra/Silvan Thoma/Martin Liebi/Urszula McCormack/Rika Khurdayan/Lee Schneider/Lewin Boehnke/Dominik Spicher/Marius Smith/Oliver Völkel/Bryan Hollmann/Andy Flury, The Security Token Report 2021, Schaan 2021

Heilman/Kendler/Zohar/Goldberg, 2015. Ethan Heilman/Alison Kendler/Aviv Zohar/Sharon Goldberg, Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In: USENIX Association (ed.), Proceedings of the 24th USENIX Security Symposium, Washington, D.C. 2015, 129–144

Hertig, 2012. Gérard Hertig, Post-financial Crisis Trading and Clearing Reforms in the EU: A Story of Interest Groups with Magnified Voice. In: Eddy Wymeersch/Klaus J. Hopt/Guido Ferrarini (Hrsg.), Financial Regulation and Supervision, Oxford 2012, 321-336

Hoeren/Prinz, 2021. Thomas Hoeren/Wolfgang Prinz, Das Kunstwerk im Zeitalter der technischen Reproduzierbarkeit – NFTs (Non-Fungible Tokens) in rechtlicher Hinsicht, CR 2021, 565–572

Hon/Palfreyman/Tegart, 2016. W. Kuan Hon/John Palfreyman/Matthew Tegart, Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector, Athens 2016

Houdrouge/Tenot, 2020. Tarek Houdrouge/Jérémie Tenot, Le droit suisse à l'heure de la technologie des registres électroniques distribués, Not@lex 2020, 49–63

Humbel, 2019. Claude Humbel, Die Regelung der Vor- und Nachhandelstransparenz in der Europäischen Union und der Schweiz, Diss. Zürich 2019

I

Iqbal/Matulevičius, 2021. Mubashar Iqbal/Raimundas Matulevičius, Exploring Sybil and Double Spending Risks in Blockchain Systems, IEEE Access 2021, 76153–76177

J

Jacquemart/Meyer, 2017. Nicolas Jacquemart/Stephan D. Meyer, Der Bitcoin-Bitcoin-Cash-Hardfork, GesKR 2017, 469–485

Janssen/Vennmanns, 2021. André U. Janssen/Tom J. Vennmanns, Smart Dispute Resolution in the Digital Age: The Potential of Smart Contracts and Online Dispute Resolution for Dispute Prevention and Resolution in Consumer Law Cases, IJCLP 2021, 52–73

Jian/Ran/Liyan, 2021. Zhou Jian/Qu Ran/Sun Liyan, Securing Blockchain Wallets Efficiently Based on Threshold ECDSA Scheme Without Trusted Center, ACCTC 2021, 47–51

Jiang/Liu/Chan, 2018. Bo Jiang/Ye Liu/Wingkwong Chan, ContractFuzzer: fuzzing smart contracts for vulnerability detection, ASE 2018: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, 259–269

Jotterand, 2022. Alexandre Jotterand, Personal Data or Anonymous Data: where to draw the lines (and why)?. In: Jusletter 15. August 2022

K

Kaal/Calcaterra, 2017. Wulf A. Kaal/Craig Calcaterra, Crypto Transaction Dispute Resolution, Business Lawyer 2017-2018, 109–152

Katsch/Rifkin/Gaitenby, 2000. Ethan Katsch/Janet Rifkin/Alan Gaitenby, E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of «eBay Law», OSJDR 2000, 705–734

Kaufmann-Kohler/Rigozzi, 2015. Gabrielle Kaufmann-Kohler/Antonio Rigozzi, International Arbitration, Law and Practice in Switzerland, 3rd ed., Oxford 2015

Kaulartz, 2016. Markus Kaulartz, Die Blockchain-Technologie, CR 2016, 474–480

Kaulartz, 2019. Markus Kaulartz, Smart Contract Dispute Resolution. In: Martin Fries/Boris P. Paal (Hrsg.), Smart Contracts, Tübingen 2019, 73–84

Kaulartz/Schmid, 2021. Markus Kaulartz/Alexander Schmid, Rechtliche Aspekte sogenannter Non-Fungible Tokens (NTFs), CB 2021, 298–302

Kedziora/Kozlowski/Jozwiak, 2020. Michal Kedziora/Patryk Kozlowski/Piotr Jozwiak, Security of Blockchain Distributed Ledger Consensus Mechanism in Context of the Sybil Attack. In: Hamido Fujita/Philippe Fournier-Viger/Moonis Ali/Jun Sasaki (eds.), Trends in Artificial Intelligence Theory and Applications, Artificial Intelligence Practices, 33rd International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Cham 2020, 407–418

Komm. NBG-*Bearbeiter/in*, 2021. Martin Plenio/Myriam Senn (Hrsg.), Nationalbankgesetz – Bundesgesetz über die Währung und die Zahlungsmittel, Kommentar, Zürich 2021

Kosseff, 2018. Jeff Kosseff, Defining Cybersecurity Law, Iowa Law Rev. 2018, 985–1031

Koula, 2016. Riika Koula, Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement, SCRIPTed 2016, 40–69

Kramer/Meier, 2020. Stefan Kramer/Urs Meier, Tokenisierung von Finanzinstrumenten, GesKR 2020, 60–77

Kramer/Oser/Meier, 2019. Stefan Kramer/David Oser/Urs Meier, Tokenisierung von Finanzinstrumenten de lege ferenda. In: Jusletter 6. Mai 2019

Kreis/Kaulartz, 2019. Falco Kreis/Markus Kaulartz, Smart Contracts and Dispute Resolution – A Chance to Raise Efficiency?, ASA Bull. 2019, 336–357

Kuhn, 2021a. Hans Kuhn, Digitale Aktiven im schweizerischen Privatrecht. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 51–129

Kuhn, 2021b. Hans Kuhn, Entwicklungen im Ausland. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 251–283

Kuhn/Stengel/Meisser/Weber, 2019. Hans Kuhn/Cornelia Stengel/Luzius Meisser/Rolf H. Weber, Wertrechte als Rechtsrahmen für die Token-Wirtschaft. In: Jusletter IT 23. Mai 2019

Kuhn/Weber, 2021. Hans Kuhn/Rolf H. Weber, Einleitung. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 1–8

L

Landbrecht/Wehowsky, 2022. Johannes Landbrecht/Andreas Wehowsky, Arbitrating Blockchain and Smart Contract Disputes – Lessons to be Learnt from Commodities and Shipping Arbitration?, ASA Bull. 2022, 309–331

Lehar/Parlour, 2021. Alfred Lehar/Christine A. Parlour, Miner Collusion and the Bitcoin Protocol, April 27, 2021, 1–38

Li/Jiang/Chen/Luo/Wen, 2020. Xiaoqi Li/Peng Jiang/Ting Chen/Xiapu Luo/Qiaoyan Wen, A Survey on the Security of Blockchain Systems, arXiv:1802.06993v3 (2020), 1–25

Li/Jiang/Li/Wang, 2022. Yuze Li/Shangrong Jiang/Xuerong Li/Shouyang Wang, Hybrid data decomposition-based deep learning for Bitcoin prediction and algorithm trading, FIN 2022. 1–24, aufrufbar unter <https://link.springer.com/content/pdf/10.1186/s40854-022-00336-7.pdf>

Low, 2020. Kelvin F.K. Low, Confronting Cryptomania: Can Equity Tame the Blockchain?, Legal Studies Research Paper No. 2020-01, Hong Kong 2020

Low/Mik, 2020. Kelvin F.K. Low/Eliza Mik, Pause the Blockchain Legal Revolution, ICLQ 2020, 135–175

M

Mader/Rütsche, 2004. Luzius Mader/Bernhard Rütsche, Regulierung, Deregulierung, Selbstregulierung: Anmerkungen aus legistischer Sicht, ZSR 2004, 1. Heft, II: Halbband, 1–156

Madir, 2019. Jelena Madir, Smart Contracts. In: Jelena Madir (ed.), FinTech, Law and Regulation, Cheltenham/Northampton 2019, 148–170

Malisa, 2017. Luka Malisa, Security of User Interfaces: Attacks and Countermeasures, Diss. ETH, Zürich 2017

Marino/Juels, 2016. Bill Marino/Ari Juels, Setting Standards for Altering and Undoing Smart Contracts, Rule Technologies – Research, Tools and Applications, Cham 2016, 151–166

Maull et al., 2017. Roger Maull/Philip Godsiff/Catherine Mulligan/Alan Brown/Elizabeth Kewell, Distributed Ledger Technology: Applications and Implications, SC 2017, 481–489

Maurenbrecher, 2005. Benedikt Maurenbrecher, Von der Investment Services Directive zur Markets in Financial Instruments Directive – ein Überblick aus Schweizer Sicht, AJP 2005, 19-38

Meier/Schuppli, 2019. Julia Meier/Benedikt Schuppli, The DAO Hack and the Living Law of Blockchain. In: Alexandra Dal Molin-Kränzlin/Anne Mirjam Schneuwly/Jasna Stojanovic (Hrsg.), Digitalisierung – Gesellschaft – Recht, Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich, Zürich/St. Gallen 2019, 27–43

Meier-Hayoz/von der Crone, 2018. Arthur Meier-Hayoz/Hans Caspar von der Crone, Wertpapierrecht, 3. Aufl., Bern 2018

Meyer/Métille, 2022. Pauline Meyer/Sylvain Métille, Loi fédérale sur la sécurité de l'information: version 2.0. In: Jusletter 5. September 2022

Monsch, 2018. Martin Monsch, Hochfrequenzhandel: Eine rechtsökonomische Analyse des Phänomens sowie eine rechtsdogmatische Betrachtung des schweizerischen Aufsichtsrechts unter funktionaler Berücksichtigung des europäischen Rechts, Diss. Zürich 2018

Montavon, 2021. Michael Montavon, Cyberadministration et protection des données, Étude théorique et pratique de la transition numérique du point de vue de l'État, des citoyen-ne-s et des autorités de contrôle, Genève/Zurich/Bâle 2021

Montavon, 2022. Michael Montavon, De la planification à la codification de la cyberadministration, SJZ 2022, 803–812

Moser, 2021. Werner Moser, Die Ombudsinstitution in der Schweiz, Zürich/Basel/Genf 2021

Mühlberger et al., 2020. Roman Mühlberger/Stefan Bachhofner/Eduardo Castelló Ferrer/Claudio Di Ciccio/Ingo Weber/Maximilian Wöhrer/Uwe Zdun, Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World, BPM 2020, 35–51

MüKo BGB-*Bearbeiter/in*. Franz Jürgen Säcker et al. (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 8. Aufl., München 2020

Mulia/Kumari, 2021. Sharath Mulia/Romi Kumari, Blockchain Arbitration: The Future of Dispute Resolution, last updated November 2021, aufrufbar unter <https://www.lexology.com/library/detail.aspx?g=2a2f2cef-39a5-4551-a7df-4c9e408a5ccc>

Müller, 2019. Christoph Müller, Die Smart Contracts aus Sicht des Schweizerischen Obligationenrechts, ZBJV 2019, 330–352

Müller/Seiler, 2019. Lukas Müller/Reto Seiler, Smart Contracts aus Sicht des Vertragsrechts, Funktionsweise, Anwendungsfälle und Leistungsstörungen, AJP 2019, 317–328

N

Nagel, 2020. Sebastian Nagel, Stabilität und Resilienz des Finanzmarkts. In: Stefanie Hiss/Agnes Fessler/Gesa Griese/Sebastian Nagel/Daniela Woschnack (eds.), Nachhaltigkeit und Finanzmarkt, Zur soziologischen Vermessung eines Reflexionsraums, Wiesbaden 2020, 143–161

Nakamoto, 2008. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, aufrufbar unter <https://bitcoin.org/bitcoin.pdf>

Nascimento/Pólvora, 2019. Susana Nascimento/Alexandre Pólvora (Hrsg.), Blockchain now and tomorrow: assessing multidimensional impacts of distributed ledger technologies, Luxembourg 2019

O

O'Shields, 2017. Reggie O'Shields, Smart Contracts: Legal Agreements for the Blockchain, NCBI 2017, 177–194

OFK FinfraG-*Bearbeiter/in*. Alexander Vogel/Christoph Heiz/Reto Luthiger (Hrsg.), FinfraG/BEG Kommentar, Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel und Bundesgesetz über Bucheffekten mit weiteren Erlassen, Zürich 2019

Ortolani, 2019. Pietro Ortolani, The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads, Unif. Law Rev. 2019, 430–448

Ortolani, 2021. Pietro Ortolani, Smart Contracts, ODR and the New Landscape of the Dispute Resolution Market. In: Benedetta Cappiello/Gherardo Carullo (eds.), Blockchain, Law and Governance, Cham 2021, 215–219

P

Pala/Alamb/Thakura/Singh, 2021. Om Pala/Bashir Alamb/Vinay Thakura/Surendra Singh, Key management for blockchain technology, ICT Express 2021, 76–80

Palombo/Battaglini/Cantisani, 2021. Alessandro Palombo/Raffaele Battaglini/Luigi Cantisani, A Blockchain-Based Smart Dispute Resolution Method. In: Larry A. Di Matteo/André Janssen/Pietro Ortolani/Francisco de Elizalde/Michel Cannarsa/Mateja Durovic (eds.), The Cambridge Handbook of Lawyering in the Digital Age, Cambridge 2021, 122–139

Patterson, 2010. Scott Patterson, The quants: how a new breed of math whizzes conquered Wall Street and nearly destroyed it, New York 2010

Patterson, 2012. Scott Patterson, Dark pools: high-speed traders, AI bandits, and the threat to the global financial system, New York 2012

Perez/Livshits, 2021. Daniel Perez/Benjamin Livshits, Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited, USENIX Association (ed.), Proceedings of the 30th USENIX Security Symposium 2021, 1325–1341, aufrufbar unter <https://2459d6dc103cb5933875-c0245c5c937c5dedcca3f1764ecc9b2f.ssl.cf2.rackcdn.com/sec21/sec21_full_proceedings.pdf>

Pérez-Solà/Delgado-Segura/Navarro-Arribas/Herrera-Joancomartí, 2019. Cristina Pérez-Solà/Sergi Delgado-Segura/Guillermo Navarro-Arribas/Jordi Herrera-Joancomartí, Double-spending prevention for Bitcoin zero-confirmation transactions, Int. J. Inf. Secur. 2019, 451–463

Q

R

Rabinovich-Einy/Katsch, 2019. Orna Rabinovich-Einy/Ethan Katsch, Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution, JDR 2019, 1–29, aufrufbar unter <https://scholarship.law.missouri.edu/jdr/vol2019/iss2/6>

Rajab et al., 2020. Tayebeh Rajab/Mohammad Hossein Manshaei/Mohammad Dakhilalian/Murtuza Jadliwala/Mohammad Ashiqur Rahman, On the Feasibility of Sybil Attacks in Shard-Based Permissionless Blockchains, arXiv:2002.06531v1, 2020, 1–10

Rauchs et al., 2018. Michel Rauchs/Andrew Glidden/Brian Gordon/Gina Pieters/Martino Recanatini/François Rostand/Kathryn Vagneur/Bryan Zhang, Distributed Ledger Technology Systems: A Conceptual Framework, Cambridge 2018

Rosenfeld, 2014. Meni Rosenfeld, Analysis of hashrate-based double-spending, arXiv:1402.2009, 2014, 1–13

Rosenthal, 2019. David Rosenthal, Löschen und doch nicht löschen, digma 2019, 190–198

Rosenthal, 2020. David Rosenthal, Das neue Datenschutzgesetz. In: Jusletter 16. November 2020

Roth/Schär/Schöpfer, 2021. Jakob Roth/Fabian Schär/Aljoscha Schöpfer, The Tokenization of Assets: Using Blockchains for Equity Crowdfunding. In: Karen Wendt (ed.), Theory of Change: Change Leadership Tools, Models and Applications for Investing in Sustainable Development, Cham 2021, 329–350

Rutishauser/Kubli/Weber, 2021. Daniel Rutishauser/Ralf Kubli/Rolf H. Weber, Grundlagen. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 9–34

S

Salmon/Myers, 2019. John Salmon/Gordon Myers, Blockchain and Associated Legal Issues for Emerging Markets, EMcompass 2019, 1–8

Saulnier/Giustacchini, 2020. Jérôme Saulnier/Ilaria Giustacchini, Digital finance: emerging risks in crypto-assets – regulatory and supervisory challenges in the area of financial services, institutions and markets, European Parliamentary Research Service, September 2020

Sayeed/Marco-Gisbert, 2019. Sarwar Sayeed/Hector Marco-Gisbert, Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack, Appl. Sci. 2019, No. 9:1788, 1–17

Schär, 2021. Fabian Schär, Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, Fed. Reserve Bank St. Louis Rev. 2021, 153–174

Schär/Berentsen, 2017. Fabian Schär/Aleksander Berentsen, Bitcoin, Blockchain und Kryptoassets, Eine umfassende Einführung, Norderstedt 2017

Schär/Berentsen, 2020. Fabian Schär/Aleksander Berentsen, Bitcoin, Blockchain, and Cryptoassets, Cambridge MA/London 2020

Schär/Hübner, 2020. Fabian Schär/Philipp Hübner, Blockchain und Smart Contracts im Kontext der Prozessautomatisierung. In: Manfred Bruhn/Karsten Hadwich (Hrsg.), Automatisierung und Personalisierung von Dienstleistungen, Berlin 2020, 297–316

Schleiffer/Schärli, 2018. *Patrick Schleiffer/Patrick Schärli*, Multilaterale Handelssysteme (MTF) und organisierte Handelssysteme (OTF). In: Peter Sester/Beat Brändli/Oliver Bartholet/Reto Schiltknecht (Hrsg.), St. Galler Handbuch zum Schweizer Finanzmarktrecht/Finanzmarktaufsicht und Finanzmarktinfrastrukturen, Zürich/St. Gallen 2018, 859-908

Schmitz/Rule, 2019. Amy J. Schmitz/Colin Rule, Online Dispute Resolution for Smart Contracts, JDR 2019, 103–125

Schultz/Sarre, 2022. Marion Schultz/Frank Sarre, Nutzung von Cloud Services im Unternehmen – Verantwortlichkeiten für die IT-Sicherheit, CR 2022, 281–291

Schurr, 2019. Francesco H. Schurr, Anbahnung, Abschluss und Durchführung von Smart Contracts im Rechtsvergleich, ZVglRWiss 2019, 257–284

Scott/Brown/Flakoll/Ossio, 2022. Kate Scott/Sam Brown/Rita Flakoll/Diego Ballon Ossio, Arbitration for Cryptoassets and Smart Contract Disputes, London 2022

Seehafer/Hillebrand, 2021. Astrid Seehafer/Sarah Hillebrand, Der Kräuterpfarrer und neue Technologien: Zur Anwendbarkeit der Produkthaftungsrichtlinie bei verkörperten geistigen Leistungen, EuZW 2021, 1032–1034

Seiler/Griesinger, 2022. Daniel W. Seiler/Marcel Griesinger, Anforderungen an die Datensicherheit nach dem revidierten Datenschutzgesetz unter besonderer Berücksichtigung der Cyber-Sicherheit. In: Jusletter IT 26. April 2022

Sester/Nitschke, 2004. Peter Sester/Tanja Nitschke, Software-Agent mit Lizenz zum ....?, Vertragsschluss und Verbraucherschutz beim Einsatz von Softwareagenten, CR 2004, 548–554

Sheldon, 2019. Mark D. Sheldon, A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit, Curr. Issues Audit. 2019, A15–A29

Singh/Hosen/Yoon, 2021. Saurabh Singh/A. S. M. Sanwar Hosen/Byungun Yoon, Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network, IEEE Access 2021, 13938–13959

Singh/Ngan/Druschel/Wallach, 2006. Atul Singh/Tsuen-Wan «Johnny» Ngan/Peter Druschel/Dan S. Wallach, Eclipse Attacks on Overlay Networks: Threats and Defenses, Joint Conference of the IEEE Computer and Communications Societies 2006, 1–12

Singha et al., 2020. Amritraj Singha/Kelly Clicka/Reza M. Parizia/Qi Zhangb/Ali Dehghantanha/Kim-Kwang Raymond Choo, Sidechain technologies in blockchain networks: An examination and state-of-the-art review, J. Netw. Comput. Appl. 2020, No. 149:102471, 1–16

Sinitsyn/Diakonova/Chursina, 2022. Sergei A. Sinitsyn/Maria O. Diakonova/Tatyana I. Chursina, Smart Contracts in the Digital Economy: Contractual Regulation and Dispute Resolution. In: Agnessa O. Inshakova/Evgenia E. Frolova (eds.), Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment, Singapore 2022, 155–164

SK FinfraG-*Bearbeiter/in*. Rolf Sethe et al. (Hrsg.), Schulthess Kommentar, Kommentar zum Finanzmarktinfrastrukturgesetz, FinfraG, Zürich/Basel/Genf 2017

Spindler, 2007. Gerald Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Studie im Auftrag des BSI, Bonn 2007

Stengel/Bianchi, 2021. Cornelia Stengel/Luca Bianchi, Geldwäscherei und Terrorismusfinanzierung. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 223–250

Swathi/Modi/Patel, 2019. Punathumkandi Swathi/Chirag Modi/Dhiren Patel, Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners, 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2019, 1–6

Szabo, 1994. Nick Szabo, Smart Contracts, 1994, aufrufbar unter <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>

Szabo, 1996. Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996, aufrufbar unter <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html>

T

Tapscott/Tapscott, 2016. Don Tapscott/Alex Tapscott, The Blockchain Revolution, How the Technology Behind Bitcoin is Changing Money, Business, and the World, Toronto 2016

Tschorsch/Scheuermann, 2016. Florian Tschorsch/Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IEEE Communications Surveys & Tutorials 2016, 2084–2123

U

Urbach et al., 2018. Nils Urbach/Gilbert Fridgen/Florian Guggenmoos/Jannik Lockl/Alexander Rieger/André Schweizer, Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process, ERCIM-Blockchain 2018, 1–8

Urien, 2021. Pascal Urien, Innovative Countermeasures to Defeat Cyber Attacks Against Blockchain Wallets, 5th CSNet Conference 2021, Abu Dhabi 2021, 49–54

V

Varmaz/Varmaz/Günther/Poddig, 2021. Armin Varmaz/Nermin Varmaz/Steffen Günther/Thorsten Poddig, Rechtliche und finanzökonomische Grundlagen. In: Sebastian Omlor/Mathias Link (Hrsg.), Kryptowährungen und Token, Frankfurt am Main 2021, 1–42

Vokerla et al., 2019. Rahul Rao Vokerla/Bharanidharan Shanmugam/Sami Azam/Asif Karim/Friso De Boer/Mirjam Jonkman/Fahad Faisal, An Overview of Blockchain Applications and Attacks, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) 2019, 1–6

Volz, 2022. Stephanie Volz, KI Sandboxen für die Schweiz?, SZW 2022, 51–68

von der Crone/Baumgartner, 2020. Hans Caspar von der Crone/Fleur Baumgartner Digitalisierung des Aktienrechts – Die Ausgabe von Aktien als Registerwertrechte, SZW 2020, 351–364

von der Crone/Derungs, 2019. Hans Caspar von der Crone/Merens Derungs, Aktien als digitalisierte Werte, SZW 2019, 481–497

von Rosenstiel, 2021. Anja von Rosenstiel, Technology as party in decentralized dispute resolution, pm 2021, 270–276

W

Wagner/Weber, 2017. Alexander F. Wagner/Rolf H. Weber, Corporate Governance auf der Blockchain, SZW 2017, 59–70

Walch, 2017. Angela Walch, The Path of the Blockchain Lexicon (and the Law), RBFL 2017, 713–765

Walker et al., 2006. Brian H. Walker/Lance H. Gunderson/Ann P. Kinzig/Carl Folke/Steve R. Carpenter/Lisen Schultz, A Handful of Heuristics and Some Propositions for Understanding Resilience in Social-Ecological Systems, Ecol. Soc. 2006, Art. 13 (online), 1–15

Wang et al., 2018. Shuai Wang/Yong Yuan/Xiao Wang/Juanjuan Li/Rui Qin/Fei-Yue Wang, An Overview of Smart Contract: Architecture, Applications, and Future Trends, IEEE Intelligent Vehicles Symposium 2018, 108–113

Weber, 1996. Rolf H. Weber, Zivilrechtliche Haftung auf dem Information Highway. In: Reto M. Hilty (Hrsg.), Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Bern 1996, 531–557

Weber, 2012. Rolf H. Weber, Overcoming the Hard Law/Soft Law Dichotomy in Times of (Financial) Crises, J. Gov. Regul. 2012, 8–14

Weber, 2014. Rolf H. Weber, Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles, Zürich 2014

Weber, 2017a. Rolf H. Weber, Regulatory Environment of the Ledger Technology, CRi 2017, 1–6

Weber, 2017b. Rolf H. Weber, Liability in the Internet of Things, EuCML 2017, 207–212

Weber, 2017c. Rolf H. Weber, Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts. In: Jusletter 4. Dezember 2017

Weber, 2018a. Rolf H. Weber, Smart Contracts: Vertrags- und verfügungsrechtlicher Regelungsbedarf?, sic! 2018, 291–301

Weber, 2018b. Rolf H. Weber, Development of Coherent Procedural Rules for OECD Guidelines Mediation. In: Nicola Bonucci/Catherine Kessedjian (Hrsg.), 40 ans des lignes directrices de l'OECD pour les entreprises multinatinales – 40 Years of the OECD Guidelines for Multinational Enterprises, Paris 2018, 101–117

Weber, 2020. Rolf H. Weber, Cybersecurity in International Law. In: Asian Academy of International Law (Ed.), 2019 Colloquium on International Law, Synergy and Security: The Keys to Sustainable Global Investment, Hong Kong 2020, 279–308

Weber, 2021a. Rolf H. Weber, Handel mit digitalen Aktiven. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 165–197

Weber, 2021b. Rolf H. Weber, Sectoral Self-Regulation as Viable Tool. In: Klaus Mathis/Avishalom Tor (eds.), Law and Economics of Regulation, Cham 2021, 25–36

Weber, 2021c. Rolf H. Weber, Zivilrechtliche Aspekte von Geschäftsabwicklungen auf DLT-Handelsplattformen, SZW 2021, 450–460

Weber, 2021d. Rolf H. Weber, Haftungsfragen beim Handel von digitalen Vermögenswerten, SJZ 2021, 679–687

Weber, 2021e. Rolf H. Weber, Neue Blockchain-Gesetzgebung in der Schweiz, RDi 4/2021, 186–195

Weber, 2022a. Rolf H. Weber, Open Finance and Decentralized Finance – Entwicklungen in einem disruptiven Finanzmarktumfeld, SZW 2022, 3–13

Weber, 2022b. Rolf H. Weber, Sicherheit und Resilienz in DLT-basierten Finanzmarktinfrastrukturen. In: Jusletter 13. Juni 2022

Weber/Baisch, 2015. Rolf H. Weber/Rainer Baisch, Optimierung der Rechtsdurchsetzung, Analyse am Beispiel des Finanzmarktrechts. In: Peter Breitschmid/Ingrid Jent-Sørensen/Hans Schmid/Miguel Sogo (Hrsg.), Festschrift für Isaak Meier zum 65. Geburtstag, Zürich/Basel/Genf 2015, 775–792

Weber/Baisch, 2019a. Rolf H. Weber/Rainer Baisch, Crowdinvesting mittels Initial Coin Offering – Regulierungsaufgaben im Token-Universum, SZW 2019, 135–154

Weber/Baisch, 2019b. Rolf H. Weber/Rainer Baisch, Internationale Entwicklungen in der Crypto-Asset-Regulierung (ICO/Token). In: Jusletter 18. Februar 2019

Weber/Baisch, 2021. Rolf H. Weber/Rainer Baisch, DLT-basierte Finanzprodukte, SZW 2021, 683–697

Weber/Baumann, 2015. Rolf H. Weber/Simone Baumann, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien. In: Jusletter 21. September 2015

Weber/Kuhn, 2021. Rolf H. Weber/Hans Kuhn, Ausblick. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 285–289

Weber/Staiger, 2017. Rolf H. Weber/Dominic N. Staiger, New Liability Patterns in the Digital Era. In: Tatiana-Eleni Synodinou et al. (eds.), EU Internet Law, Regulation and Enforcement, Cham 2017, 197–214

Weber/Studer, 2016. Rolf H. Weber/Evelyne Studer, Cybersecurity in the Internet of Things: Legal aspects, CLSR 2016, 715–728

Weber/Wolf, 2012. Rolf H. Weber/Christoph Wolf, Fragmentarische E-Commerce Gesetzgebung. In: Jusletter 18. Juni 2012

Weber/Yildiz, 2021. Rolf H. Weber/Okan Yildiz, Alternative Dispute Resolution auf DLT-Handelsplattformen. In: Jusletter 14. Juni 2021

Weber/Yildiz, 2022. Rolf H. Weber/Okan Yildiz, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, Zürich 2022

Webley/Hardy, 2015. Tom Webley/Peter Hardy, What Can Be Done to Mitigate Cyber Risk?, JIBFL 2015, 353–357

Wen/Lu/Liu/Huang, 2021. Yujuan Wen/Fengyuan Lu/Yufei Liu/Xinli Huang, Attacks and countermeasures on blockchains: A survey from layering perspective, Comp. Netw. 2021, 107978, 1–17

Werbach/Cornell, 2017. Kevin Werbach/Nicolas Cornell, Contracts Ex Machina, Duke L.J. 2017, 313–382

Wyss, 2019. Dominic Wyss, Gegenstand und Übertragung von DLT-Wertrechten. In: Jusletter 1. Juli 2019

X

Y

Z

Zellweger-Gutknecht/Monnerat, 2021. Corinne Zellweger-Gutknecht/Lucien Monnerat, Internationaler Kontext: schweizerische Registerwertrechte. In: Sebastian Omlor/Florian Möslein/Stefan Grundmann (Hrsg.), Elektronische Wertpapiere, Tagungsband, Tübingen 2021, 7–32

Zellweger-Gutknecht/Weber, 2022. Corinne Zellweger-Gutknecht/Rolf H. Weber, Digital Money – Taxonomy and Regulatory Approaches, EuZ 2022, G 1–G 34

Zetzsche/Anker-Sørensen/Passador/Wehrli, 2022. Dirk Zetzsche/Linn Anker-Sørensen/Maria Lucia Passador/Andreas Wehrli, DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective, BIS Working Papers No 1015 of 20 May 2022

Zetzsche/Annunziata/Arner/Buckley, 2021. Dirk A. Zetzsche/Filippo Annunziata/Douglas W. Arner/Ross P. Buckley, The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy, Cap. Mark. Law J. 2021, 203-225

Zetzsche/Buckley/Arner/Föhr, 2019. Dirk A. Zetzsche/Ross P. Buckley/Douglas W. Arner/Linus Föhr, The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators, Harv. Int. Law J. 2019, 267-315

Zetzsche/Woxholth, 2022. Dirk A. Zetzsche/Jannik Woxholth, The DLT Sandbox under the Pilot-Regulation, Cap. Mark. Law J. 2022, 212–236

Zhang/Lee, 2019. Shijie Zhang/Jong-Hyouk Lee, Double Spending With a Sybil Attack in the Bitcoin Decentralized Network, IEEE Transactions on Industrial Informatics 2019, 5715–5722

Zimmermann, 2012. Heinz Zimmermann, Effektenhandel im technologischen und regulatorischen Umbruch. In: Brigitte Strebel-Aerni (Hrsg.), Finanzmärkte im Banne von Big Data, Zürich 2012, 95-136

Zobl/Kramer, 2004. Dieter Zobl/Stefan Kramer, Schweizerisches Kapitalmarktrecht, Zürich/Basel/Genf 2004

Materialienverzeichnis

Alle Internet-Dokumente sind letztmals am 21. Februar 2022 besucht worden.

AFCA, 2021. Australian Financial Complaints Authority (AFCA), Complaint Resolution Scheme Rules of 13 January 2021, aufrufbar unter <https://www.afca.org.au/media/1111/download>

Bitcoinsuisse, 2020. Bitcoinsuisse, Was ist Staking? Eine neue Art, Kryptowährungen zu verdienen, Zug 2020, aufrufbar unter <https://www.bitcoinsuisse.com/de/news/was-ist-staking>

Botschaft DLT-Gesetz, BBl 2020. Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, BBl 2020, 233 ff., aufrufbar unter <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/16/de/pdf-a/fedlex-data-admin-ch-eli-fga-2020-16-de-pdf-a.pdf>

Botschaft FinfraG, BBl 2014. Botschaft zum Finanzmarktinfrastrukturgesetz (FinfraG) vom 3. September 2014, BBl 2014, 7483 ff., aufrufbar unter <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2014/1633/de/pdf-a/fedlex-data-admin-ch-eli-fga-2014-1633-de-pdf-a.pdf>

Botschaft GwG, BBl 2019. Botschaft zur Änderung des Geldwäschereigesetzes vom 26. Juni 2019, BBl 2019, 5451 ff., aufrufbar unter <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2019/1932/de/pdf-a/fedlex-data-admin-ch-eli-fga-2019-1932-de-pdf-a.pdf>

Botschaft IPRG, BBl 2018. Botschaft zur Änderung des Bundesgesetzes über das Internationale Privatrecht (12. Kapitel: Internationale Schiedsgerichtsbarkeit) vom 24. Oktober 2018, BBl 2018, 7163 ff., aufrufbar unter <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2018/2548/de/pdf-a/fedlex-data-admin-ch-eli-fga-2018-2548-de-pdf-a.pdf>

Bundesrat, 2014. Bundesrat, Bericht des Bundesrats vom 25. Juni 2014 zu virtuellen Währungen in Beantwortungen der Postulate Schwaab (13.3687) und Weibel (13.4070), abrufbar unter: www.admin.ch > Dokumentation > Medienmitteilungen (Medienmitteilung vom 25. Juni 2014)

Bundesrat, 2018. Bundesrat, Bericht des Bundesrates vom 14. Dezember 2018 über rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf dem Finanzsektor, Bern, 14. Dezember 2018, aufrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf>

Bundesrat, 2021. Bundesart. Änderung der Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Erläuternder Bericht zur Vernehmlassungsvorlage, Bern 1. Oktober 2021, aufrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/68406.pdf>

EDSB, 2021. Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme 6/2021 zu dem Vorschlag für eine Pilotregelung für auf der Distributed-Ledger-Technologie basierende Marktinfrastrukturen vom 23. April 2021, aufrufbar unter <https://edps.europa.eu/system/files/2021-06/2021-0219_d0912_opinion_on_pilot_regime_for_market_infrastructures_de.pdf>

EFD, 2018. Eidgenössisches Finanzdepartement, Revision der Bankenverordnung (BankV) «FinTech-Bewilligung» – Erläuterungen, 30. November 2018, aufrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/54881.pdf>

EFD, 2021. Eidgenössisches Finanzdepartement, Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register – Erläuterungen, 18. Juni 2021, aufrufbar unter <https://www.newsd.admin.ch/newsd/message/attachments/67150.pdf>

ESMA/EBA/EIOPA, 2018. ESMA/EBA/EIOPA Report, FinTech: Regulatory sandboxes and innovation hubs (JC 2018 74), aufrufbar unter <https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf>

Europäische Kommission, Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung vom 19.02.2020, COM(2020) 64 final, aufrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0064&from=DE>

Europäische Kommission, Impact Assessment, 2020. European Commission, Commission staff working document, impact assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, SWD(2020) 380, aufrufbar unter <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0380>

EZB, 2017. Europäische Zentralbank (EZB), The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration, Frankfurt am Main 2017, aufrufbar unter <https://www.ecb.europa.eu/paym/groups/ami/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf>

FCA, 2017. Financial Conduct Authority, Regulatory sandbox lessons learned report, 2017, 4, aufrufbar unter <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>

FINMA, 2013a. Eidgenössische Finanzmarktaufsicht FINMA, FINMA-Rundschreiben 2013/8, Marktverhaltensregeln, Aufsichtsregeln zum Marktverhalten im Effektenhandel vom 29. August 2013 (Stand 4. November 2020), aufrufbar unter <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2013-08-01012021_de.pdf?sc_lang=de>

FINMA, 2013b. Eidgenössische Finanzmarktaufsicht FINMA, FINMA-Rundschreiben 2013/08 «Marktverhaltensregeln» – Bericht der FINMA über die Anhörung vom 27. März bis zum 13. Mai 2013 zum totalrevidierten Rundschreiben «Marktverhaltensregeln», vom 29. August 2013, aufrufbar unter <https://www.finma.ch/~/media/finma/importiertedokumente/regulierung/anhoerungen/08-rundschreiben-marktverhaltensregeln/br-rs-marktverhaltensregeln-13-8.pdf?sc_lang=de&hash=A67F57B3764AA8A278977B0C4233A08C>

FINMA, 2017a. Eidgenössische Finanzmarktaufsicht FINMA, FINMA-Aufsichtsmitteilung 04/2017, Aufsichtsrechtliche Behandlung von Initial Coin Offerings vom 29. September 2017, aufrufbar unter <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf?la=de>

FINMA, 2017b. Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2017/1, Corporate Governance – Banken, vom 22. September 2016 (Stand 4. November 2020), aufrufbar unter <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-01-20200101.pdf?sc_lang=de&hash=460F262EDC28F5497482BE0C690746A9>

FINMA, 2018a. Eidgenössische Finanzmarktaufsicht FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, aufrufbar unter <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=de&hash=95F3DDE91518C2D0D736C6C885DB8F64>

FINMA, 2018b. Eidgenössische Finanzmarktaufsicht FINMA, FINMA- Rundschreiben 2018/1, Organisierte Handelssysteme, Pflichten von Betreibern eines organisierten Handelssystems (OHS), vom 1. Januar 2018 (Stand 4. November 2020), aufrufbar unter <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-01.pdf?sc_lang=de>

FINMA, 2021a. Eidgenössische Finanzmarktaufsicht FINMA, Mindestgliederung für den Prüfbericht betreffend das Bewilligungsgesuch für ein um Bewilligung ersuchendes Institut, FINMA Berichtsvorlage, Bern 2021, aufrufbar unter <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/pruefbericht-dlths-institutsbewilligung.pdf?la=de>

FINMA, 2021b. Eidgenössische Finanzmarktaufsicht FINMA, Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem nach Art. 73a ff. Finanzmarktinfrastrukturgesetz vom 2. August 2021, Bern 2021, aufrufbar unter <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/w_dlt-handelssystem_20210802_de.pdf?sc_lang=de&hash=FF56D6E6916BC81B1CE301CD79AF65FC>

FINMA, 2022. Eidgenössische Finanzmarktaufsicht FINMA, Teilrevision der Geldwäschereiverordnung der FINMA (GwV-FINMA) – Erläuterungsbericht vom 8. März 2022, aufrufbar unter <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20220308—gwv—finma/20220308_anhoerung_gwv_finma_erlaeuterungsbericht.pdf?sc_lang=de>

IOSCO, 2020. International Organization of Securities Commissions (IOSCO), Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, Final Report, Februar 2020, aufrufbar unter <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf>

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity, Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité

OECD, 2011. Organisation for Economic Co-operation and Development (OECD), OECD Guidelines for Multinational Enterprises, 2011 Edition, Paris 2011, aufrufbar unter <https://www.oecd.org/daf/inv/mne/48004323.pdf>

PwC/CVA, 2020. PricewaterhouseCoopers International/Crypto Valley Association, 6th ICO / STO Report, Zurich 2020, aufrufbar unter <https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf>

Resilient, 2020. Resilient, Towards Resilient EU HPC Systems: A Blueprint, European HPC resilience initiative, 2020, aufrufbar unter <https://resilienthpc.eu/sites/default/files/pdf/Blueprint2020__Towards-Resilient-EU-HPC-Systems.pdf>

SBF, 2021a. Swiss Blockchain Federation, Circular 2019/01, Tokenized Equity – Guidelines for Issuers of Equity and Related Tokens – Updated Version of October 2021, aufrufbar unter <https://blockchainfederation.ch/wp-content/uploads/2021/11/Circular-2019_01_Updated_Tokenized-Equity.pdf>

SBF, 2021b. Swiss Blockchain Federation, Circular 2020/01, Secondary Markets for Security Tokens – Updated Version of September 2021, aufrufbar unter <https://blockchainfederation.ch/wp-content/uploads/2021/10/SBF-2020-01_Secondary_Markets_for_Digital_Securities_2021-10-12.pdf>

SBF, 2021c. Swiss Blockchain Federation, Zirkular 2021/01, Registerwertrechte – Update vom September 2021, aufrufbar unter <https://blockchainfederation.ch/wp-content/uploads/2022/09/Zirkular-2021_01-Registerwertrechte.pdf>

SCA, 2021. Swiss Crowdfunding Association, Security Token Offerings in Switzerland, A new form of crowdfunding, White Paper 2021, Geneva 2021, aufrufbar unter <https://www.swisscrowdfundingassociation.ch/wp-content/uploads/2021/04/SCA_White_Paper_2021.pdf>

UNCITRAL, 2016. United Nations Commission on International Trade Law (UNCITRAL), Report of Working Group III (Online Dispute Resolution) on the work of its thirty-third session (New York, 29 February–4 March 2016), A/CN.9/868, aufrufbar unter <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/014/73/PDF/V1601473.pdf?OpenElement>

UNCITRAL, 2017. United Nations Commission on International Trade Law (UNCITRAL), Technical Notes on Online Dispute Resolution, New York 2017, aufrufbar unter <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/v1700382_english_technical_notes_on_odr.pdf>

UVEK, 2020. Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK), Regulatory Sandboxes – Best Practices für die Schweiz, Freiräume für neue Lösungen und digitale Innovation in der Stromversorgung, Bericht vom 28. Februar 2020, aufrufbar unter <https://pubdb.bfe.admin.ch/de/publication/download/10074>

WEF, 2020. World Economic Forum, Bridging the Governance Gap: Dispute resolution for blockchain-based transactions, White Paper, December 2020, aufrufbar unter <https://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf>

Wolrd Bank Group, 2017. World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note, No. 1, Washington 2017, aufrufbar unter <https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>

Abkürzungsverzeichnis

a.M.	anderer Meinung
AAA	American Arbitration Association
ABl.	Amtsblatt der Europäischen Union (Brüssel)
Abs.	Absatz
ACCTCS	Asia-Pacific Conference on Communications Technology and Computer Science
ACM	Association for Computing Machinery
ADR	Alternative Dispute Resolution
aDSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1, Stand am 1. März 2019)
AJP/PJA	Aktuelle Juristische Praxis/Pratique Juridique Actuelle (Zürich)
ALR	Arbitration Law Review (Pennsylvania)
AML	Anti Money Laundering
Anwaltsrevue	Anwaltsrevue – das Praxismagazin des Schweizerischen Anwaltsverbandes (Bern)
API	Application Programming Interface
Appl. Sci.	Applied Sciences (Basel)
Arbitr. Int.	Arbitration International (London)
Art.	Artikel
ASA Bull.	Bulletin – Association suisse de l'arbitrag (Den Haag)
ASE	Automated Software Engineering
BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (SR 952.0; Stand am 1. August 2021)
BankV	Verordnung über die Banken und Sparkassen vom 30. April 2014 (SR 952.02; Stand am 1. August 2021)
BPM	Business Process Management: Blockchain and Robotic Process Automation Forum
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
Cap. Mark. Law J.	Capital Markets Law Journal (Oxford)
CB	Compliance-Berater (Frankfurt am Main)
CCS	Computer and Communications Security
CIETAC	China International Economic and Trade Arbitration Commission
CLSR	Computer Law & Security Review (Amsterdam/London)
Comp. Netw.	Computer Networks (Amsterdam)
CR	Computer und Recht. Zeitschrift für die Praxis des Rechts der Informationstechnologie (Köln)
CRi	Computer Law Review International, Computer und Recht International (Köln)

CSDR	Verordnung (EU) Nr. 909/2014 des Europäischen Parlamentes und des Rates zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 vom 23. Juli 2014, ABl. L 257, 1–72
CSNet	Cyber Security in Networking Conference
Curr. Issues Audit.	Current Issues in Auditing (Sarasota, FL)
CyRV	Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung vom 27. Mai 2020 (SR 120.73, Stand am 1. April 2021)
d.h.	das heisst
DeFi	Decentralized Finance
digma	digma. Schriften zum Datenrecht (Zürich; bis 2020)
DLT	Distributed Ledger-Technologie
dt.	deutsch
Duke L.J.	Duke Law Journal (Durham)
E-	Entwurf
EBK	Eidgenössischen Bankenkommission
ed./eds.	edition; editor(s)
EDR	External Dispute Resolution
EDSB	Europäischer Datenschutzbeauftragter
EMcompass	Emerging Marktes Compass (Washington)
E-MICA	Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM(2020) 593 final
engl.	englisch
ERCIM	European Research Consortium for Informatics and Mathematics
ETF	Exchange Traded Fund
ETP	Exchange Traded Products
EuCML	Journal of European Consumer and Market Law (München)
EU-DLT-Pilotregelung	Verordnung (EU) 2022/858 des Europäischen Parlaments und des Rates über eine Pilotregelung für auf Distributed-Ledger-Technologie basierende Marktinfrastrukturen und zur Änderung der Verordnungen (EU) Nr. 600/2014 und (EU) Nr. 909/2014 sowie der Richtlinie 2014/65/EU vom 30. Mai 2022, ABl. L 151, 1–33
EuZ	Zeitschrift für Europarecht (Zürich)
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (München)
EZB	Europäische Zentralbank
FDRC	Financial Dispute Resolution Centre
Fed. Reserve Bank St. Louis Rev.	Federal Reserve Bank of St. Louis Review (St. Louis)
FIDLEG	Bundesgesetz über die Finanzdienstleistungen vom 15. Juni 2018 (SR 950.1; Stand am 1. August 2021)
FIDReC	Financial Industry Dispute Resolution Centre

FIEA	Financial Instruments and Exchange Act, Act No. 25 of April 13, 1948 (englische Übersetzung aufrufbar unter <https://www.japaneselaw-translation.go.jp/en/laws/view/2355/en>
FIN	Financial Innovation (Heidelberg)
FinfraG	Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015 (SR 958.1; Stand am 1. August 2021)
FinfraV	Verordnung über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 25. November 2015 (SR 958.11; Stand am 1. Oktober 2021)
FINIV	Verordnung über die Finanzinstitute vom 6. November 2019 (SR 954.11; Stand am 1. August 2021)
FINMA	Eidgenössische Finanzmarktaufsicht
FINMAC	Financial Instruments Mediation Assistance Center
FINRA	Financial Industry Regulatory Authority
Fn.	Fussnote(n)
FOS	Financial Ombudsman Service
Future Internet	Future Internet (Basel)
GesKR	Schweizerische Zeitschrift für Gesellschafts- und Kapitalmarktrecht (Zürich)
GLJ	German Law Journal (Stuttgart)
GwG	Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 10. Oktober 1997 (SR 955.0; Stand am 1. Januar 2022)
GwV	Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 11. November 2015 (SR 955.01; Stand am 1. August 2021)
Harv. Int. Law J.	Harvard International Law Journal (Cambridge, MA)
Harv. Negot. Law Rev.	Harvard Negotiation Law Review (Cambridge, MA)
HFT	High Frequency Trading
Hrsg.	Herausgeber(in)
ICCCNT	International Conference on Computing, Communication and Networking Technologies
ICLQ	International & Comparative Law Quarterly (London)
ICO	Initial Coin Offering
ICT Express	Information & Communications Technology Express (Amsterdam)
IEEE	Institute of Electrical and Electronics Engineers
IJCLP	International Journal on Consumer Law and Practice (Bangalore)
inkl.	inklusive
Int. J. Inf. Secur.	International Journal of Information Security (Berlin)
IOSCO	International Organization of Securities Commissions
Iowa Law Rev.	Iowa Law Review (Iowa City)
ITDR	Institution for IT and Data Dispute Resolution
J. Gov. Regul.	Journal of Governance and Regulation (Sunny)

J. Int. Dispute Settl.	Journal of International Dispute Settlement (Oxford)
J. Leg. Stud.	The Journal of Legal Studies (Chicago)
J. Netw. Comput. Appl.	Journal of Network and Computer Applications (London)
J. Risk Manag. Financ. Inst.	Journal of Risk Management in Financial Institutions (London)
JDR	Journal of Dispute Resolution (Colombia)
JIBFL	Journal of International Banking and Financial Law (London)
KAG	Bundesgesetz über die kollektiven Kapitalanlagen vom 23. Juni 2006 (SR 951.31; Stand am 1. Januar 2020)
KI	künstliche Intelligenz
KYC	know your customer
m.w.H.	mit weiteren Hinweisen
MiCA-Verordnung	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM/2020/593
MiFID	Richtlinie 2014/65 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92 und 2011/61 vom 15. Mai 2014, ABl. L 173, 349–496
MiFIR	Verordnung 600/2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung 648/2012 vom 15. Mai 2014, ABl. L 173, 84–148
MMR	Multimedia und Recht (München)
Mrd.	Milliarden
MTF	Multilateral Trading Facility
NBG	Bundesgesetz über die Schweizerische Nationalbank vom 3. Oktober 2003 (SR 951.11; Stand am 1. August 2021)
NCBI	North Carolina Banking Institute (Chapel Hill)
nDSG	Bundesgesetz über den Datenschutz vom 25. September 2020 (BBl 2020, 7639 ff.) (voraussichtliches Inkrafttreten: 1. September 2023)
NFT	Non-Fungible Token
No.	Number
NYC	New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche vom 10. Juni 1958
NZZ	Neue Zürcher Zeitung
ODR	Online Dispute Resolution
ODR-Verordnung	Verordnung (EU) Nr. 524/2013 des Europäischen Parlamentes und des Rates über die Online-Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG vom 21. Mai 2013, ABl. L 165, 1–12
OECD	Organisation for Economic Co-operation and Development
OSJDR	Ohio State Journal on Dispute Resolution (Columbus)
Perform. Evaluation	Performance Evaluation (Amsterdam)
pm	Perspektive Mediation, Beiträge zur Konfliktkultur (Wien)
PrHG	Bundesgesetz über die Produktehaftpflicht vom 18. Juni 1993 (SR 221.112.944; Stand am 1. Juli 2010)

RBFL	Review of Banking & Financial Law (Boston)
RDi	Recht Digital (München)
Rz.	Randziffer(n)
S&R	Sicherheit & Recht. Sécurité & Droit. Die juristische Fachzeitschrift für Sicherheitsfragen in den Bereichen Polizei, Militär, Umwelt und Technik (Zürich)
SC	Strategic Change (Chichester, West Sussex)
SCA	Swiss Crowdfunding Association
SCRIPTed	SCRIPTed, A Journal of Law, Technology & Society (Edinburgh)
SEC	Securities and Exchange Commission
sec.	section
SHIAC	Shanghai International Economic and Trade Arbitration Commission Shanghai International Arbitration Center
SIGSAC	Special Interest Group on Security, Audit and Control
SJZ	Schweizerische Juristen-Zeitung (Zürich)
sog.	sogenannt
Stanford JBLP	Stanford Journal of Blockchain Law & Policy (Stanford)
STO	Securities Token Offering
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (Zürich)
TCCE	Trends in Computational and Cognitive Engineering
TGE	Token Generating Events
TVTG	Gesetz über Token und VT-Dienstleister vom 3. Oktober 2019 (LR-Nr. 950.6; Stand am 1. Januar 2020)
u.a.	unter anderem
UNCITRAL	United Nations Commission on International Trade Law
Unif. Law Rev.	Uniform Law Review; Revue de droit uniforme (Oxford)
Univ. Pa. Law Rev.	University of Pennsylvania Law Review (Philadelphia)
USENIX	USENIX, The Advanced Computing Systems Association
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986 (SR 241; Stand am 1. Januar 2022)
VE-	Vorentwurf
ViTECoN	Vision Towards Emerging Trends in Communication and Networking
WEF	World Economic Forum
WPES	Workshop on Privacy in the Electronic Society
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins (Bern)
ZVglRWiss	Zeitschrift für Vergleichende Rechtswissenschaft (Frankfurt am Main)

I. Einleitung

Die Digitalisierung ist ein zentraler Faktor der Innovation und der Anpassung von Geschäftsmodellen in der Volkswirtschaft. Ein erster Schub von neuen technologischen Möglichkeiten ist vor 30 Jahren mit der Einführung des Internets erfolgt. Die Distributed Ledger-Technologie[1] (DLT, in der Terminologie des Bundesrates: die Technik verteilter elektronischer Register) und die Blockchain Technologie (als umgangssprachlich oft verwendete Begrifflichkeit für eine mögliche DLT-Ausgestaltung) haben in den letzten Jahren zu stark veränderten Infrastrukturen im digitalen Bereich geführt.

Diese neuen Technologien tragen sowohl im Finanzsektor als auch in anderen Wirtschaftssektoren zu einem erheblichen, wenn auch noch nicht abschliessend abschätzbaren Innovations- und Effizienzsteigerungspotential bei. Der Regulator und der Gesetzgeber haben mit Anpassungen der regulatorischen Rahmenbedingungen für FinTech Geschäftsmodelle (Revision der BankV von 2017, Revision des BankG von 2019) relativ schnell reagiert.

Im Grundsatz beabsichtigen Politik und Recht, für optimale und innovationsfreundliche Rahmenbedingungen zu sorgen, damit die neuen Technologien den Bedürfnissen der Gesellschaft und des Marktes gerecht zu werden vermögen. Im Finanzmarktbereich gilt für die Schweiz ein prinzipienbasierter und technologieneutraler Rechtsetzungs- und Regulierungsansatz; zudem sollen die Gesetzesbestimmungen möglichst wettbewerbsneutral ausgestaltet sein. Diese Prinzipien gelten auch für auf der DLT basierende Geschäftsmodelle.

Dass ein regulatorischer Handlungsbedarf mit Blick auf die an Bedeutung gewinnenden digitalen Werte besteht, hat der Bundesrat bereits im Jahre 2018 erkannt (Bericht vom 7. Dezember 2018 zu den rechtlichen Rahmenbedingungen von Blockchain und Distributed Ledger-Technologie). Am 1. Februar 2021 (OR-Bestimmungen) und am 1. August 2021 (übrige Regelungen) ist in der Schweiz das Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen

[1] Nachfolgend werden – trotz grammatikalischer Ungenauigkeit – die englischen Begriffe ohne Bindestrich eingedeutscht und grossgeschrieben, da dies der Herangehensweise des Bundesrats entspricht und die Grossschreibung in der deutschen Sprache üblich ist. Zudem verzichten die Autoren auf spezielle Hervorhebung der englischen Ausdrücke (z.B. kursiv, Anführungszeichen). Dieser Ansatz strebt eine Einheitlichkeit innerhalb des vorliegenden Buches an und soll dem Lesefluss dienen.

der Technik verteilter elektronischer Register (DLT-Gesetz) sowie die zugehörige Mantelverordnung in Kraft getreten. Mit dieser gesetzlichen Grundlage soll den Bedürfnissen der neuen Technologien angemessen Rechnung getragen werden.

Das DLT-Gesetz hat über weite Strecken eine sinnvolle rechtliche Rahmenordnung, die es zur sicheren Abwicklung von Handelstransaktionen bedarf, geschaffen. Insoweit spielen verschiedene Aspekte eine wichtige Rolle: (i) *Zuordnung*: Die Umschreibung der digitalen Vermögenswerte hat in einer Weise zu erfolgen, dass die Zuordnung zum/zur Berechtigten möglich ist und diese Zuordnung durch Transaktionsvorgänge nicht beeinträchtigt wird. (ii) *Registrierung*: Die digitalen Vermögenswerte müssen in einer Weise festgelegt sein, dass die Zuordnung zum/zur Berechtigten zweifelsfrei und sicher (z.B. auf einem Wertrechteregister) erfolgt, und zwar auf Basis harmonisierter technischer Standards. (iii) *Verwahrung*: Der/die Berechtigte muss jederzeit Zugriff auf verwahrte digitale Vermögenswerte haben und neue Handelstransaktionen auslösen können.

Nachfolgend werden in einem ersten Schritt die technologischen Grundlagen und das Konzept der DLT aufgearbeitet; im Fokus steht dabei die Unterscheidung zwischen Blockchain und DLT sowie die Erklärung der verschiedenen Konsensmechanismen, der Wallets, des Smart Contract und der Oracles. Diese Untersuchungen dienen als Grundlage für das Verständnis der übrigen Kapitel (II.). Danach wird die regulatorische Rahmenordnung für DLT-Handelsplattformen in der Schweiz erläutert. Einerseits geht es um die (neuen) Begriffe im Rahmen der DLT (DLT-Effekte, Wertrechteregister, DLT-Handelssysteme), andererseits um die Besonderheiten im Kontext der DLT-Handelssysteme (und darüber hinaus der alternativen Handelssysteme); da der Einsatz von Algorithmen im Rahmen der DLT-Handelsplattformen bedeutungsvoll sein könnte, werden diese ergänzend ebenfalls analysiert (III.).

Weil im Rahmen der DLT-Entwicklungen neue Risiken entstehen, sind auch die Sicherheit und Resilienz bei DLT-Handelsplattformen zu beleuchten sowie die DLT-spezifischen Herausforderungen darzulegen. Ausserdem geht das Kapitel auf potenziell erforderliche Vorkehren im Rahmen der regulatorischen Vorgaben ein und macht Empfehlungen gestützt auf den gegenwärtigen Wissensstand (IV.). Hernach wird die korrekte Abwicklung von DLT-Handelstransaktionen näher betrachtet; hierfür greift dieses Buch zunächst auf die Erkenntnisse der vorangehenden Kapitel zurück und erläutert die vertragsrechtlichen Aspekte von Geschäftsabwicklungen auf DLT-Handelsplattformen im Detail. Anschliessend werden die haftungsrechtlichen Aspekte, die bei der Abwicklung

von DLT-Handelstransaktionen entstehen, näher untersucht (V.). Da auch bei DLT-basierten Transaktionen rechtliche Streitigkeiten nicht auszuschliessen sind und die staatlichen Gerichte in der Regel über wenig Erfahrungen in DLT-Fragen verfügen dürften, ist in einem letzten Schritt die Ausgestaltung der alternativen Streitschlichtung im Rahmen der DLT herauszuarbeiten (VI.). Das Buch schliesst mit einem Ausblick (VII.).

II. Digitalisierung als Innovationsfaktor und Grundlage neuer Geschäftsmodelle

Mit dem DLT-Gesetz hat der Schweizer Gesetzgeber eine neue rechtliche Rahmenordnung für die Distributed Ledger-Technologie (DLT) geschaffen. Deshalb sind zuerst die technologischen Grundlagen darzustellen; dies erweist sich als erforderlich, weil das neue Gesetz ein konzeptionelles Verständnis der DLT bzw. Blockchain-Technologie voraussetzt.

In einem ersten Schritt werden die technologischen Merkmale der DLT, d.h. die Begriffe und grundlegenden Ziele der DLT, näher erläutert (Kap. A.). Hernach ist das Grundkonzept der DLT zu erklären und darzulegen, welche Vorteile diese neue Technologie aufweist (Kap. B.). Schliesslich wird auf die Anwendungsfälle und die Bedeutung der DLT für die Wirtschaft eingegangen (Kap. C.).

A. Technologische Merkmale

In der (juristischen) Literatur fehlt oft das Bewusstsein, dass die Begriffe der DLT und der Blockchain zu unterscheiden sind. Aus diesem Grund werden vorerst diese Begriffe erläutert, um hernach den Mehrwert bzw. die grundlegenden Ziele der DLT aufzuzeigen.

1. Begriffe

Die DLT bezieht sich auf ein Konzept, das die Aufzeichnung und gemeinsame Nutzung von Daten in mehreren Datenspeichern (oder Ledgers) erlaubt. Sie ermöglicht somit die Aufzeichnung, gemeinsame Nutzung und Synchronisierung von Transaktionen und Daten über ein verteiltes Netzwerk mit verschiedenen Teilnehmenden. Die Distributed Ledgers (dt. verteilte Register) sind in der Regel öffentliche Datenbanken, verteilt auf mehrere Standorte, Länder und Institutionen. Die DLT lässt sich somit als eine spezielle Form der dezentralen Datenspeicherung und -verarbeitung (z.B. Aufzeichnung von Transaktionen) zusammenfassen, die auf einer Peer-to-Peer-Basis aufgebaut ist und ohne Intermediäre, d.h. ohne zentrale Kontrolle, funktioniert.[2]

[2] *Baker/Werbach*, 2019, Rz. 6.05 f.; *Maull et al.*, 2017, 483 f.

Die Blockchain (wörtlich: Kette von Datenblöcken)[3] ist eine spezielle Art der Datenstruktur, die in einigen Distributed Ledgers verwendet wird. Neue Daten (in der Regel Transaktionen) werden – nachdem sie von den Teilnehmenden validiert wurden – auf der Blockchain jeweils am Ende einer gegebenen Datenstruktur blockweise und chronologisch angehängt bzw. gespeichert und sind dadurch in einer digitalen Kette miteinander verbunden.[4] Blockchains verwenden kryptografische und algorithmische Methoden zur Aufzeichnung und Synchronisierung von Daten über ein Netzwerk; die Blöcke sind also durch kryptografische Hashs[5] miteinander verbunden. Jeder neu angefügte Block nimmt Bezug auf den vorherigen Block; mit diesem Prozess stellt die Technologie sicher, dass eine eindeutige und nachvollziehbare Kette von Blöcken entsteht.[6]

Die Distributed Ledgers sind eine weiter gefasste Umschreibung verteilter, synchronisierter und kryptografisch gesicherten Datenbanken.[7] Deshalb ist es in manchen Situationen erforderlich, von Distributed Ledgers und nicht Blockchain zu sprechen, da nicht alle Distributed Ledgers die Daten in miteinander verbundenen Ketten von Blöcken aufzeichnen und speichern. In diesen Fällen weisen die Distributed Ledgers u.a. nicht dieselbe sog. «Unabänderlichkeit» auf wie die Blockchains.[8]

3 *Wagner/Weber*, 2017, 59.

4 *Baker/Werbach*, 2019, Rz. 6.07; *Ganne*, 2018, 6; *Tapscott/Tapscott*, 2016, 75; *Weber/Baumann*, 2015, Rz. 26.

5 Ein kryptografischer Hash ist ein kryptografischer Fingerabdruck. Beim Hash-Algorithmus wird über eine Dateneingabe beliebiger Länge ein deterministisches Ergebnis einer fixen Länge erzeugt. Für eine spezifische Eingabe bleibt der resultierende Hashwert immer gleich und ist von allen Personen, die denselben Hash-Algorithmus verwenden, überprüfbar. Rechnerisch ist es unmöglich, eine Kollision zu provozieren, d.h. es ist unmöglich, mit zwei unterschiedlichen Eingaben denselben kryptografischen Fingerabdruck zu erzeugen (vgl. *Antonopoulos*, 2017a, 228).

6 *Low/Mik*, 2020, 137 f.; *Baker/Werbach*, 2019, Rz. 6.07; *Weber*, 2017a, 1 ff.

7 *Maull et al.*, 2017, 483.

8 *Low*, 2020, 7; *Low/Mik*, 2020, 138 m.w.H. (insb. Fn. 23).

2. Grundlegende Ziele der DLT

Die Distributed Ledger als riesiges Register, auf dem dezentrale Transaktionen registriert werden können, will sicherstellen, dass jederzeit auf allen verteilten Nodes (dt. Netzknoten) dieselben Daten gespiegelt sind. Dieser Umstand wird als technologischer Vorteil angesehen und soll die Double Spending-Problematik[9] und Manipulierbarkeit von Transaktionen einschränken.

Im Gegensatz zum World Wide Web, dem «Internet der Informationen», stehen bei der DLT (und der Blockchain), dem «Internet der Werte», die digital repräsentierten Werte, deren Besitz, der Zugang zu diesen und Transaktionen mit diesen Werten im Zentrum. Dieser Wandel ist möglich, da mit den kryptografischen Verfahren die Double Spending-Probleme auf ein Minimum begrenzt werden können. Anders als im World Wide Web lässt sich auf DLT-Systemen (bzw. der Blockchain) eindeutig feststellen, wer der rechtmässige Besitzer eines Wertes ist.

Darüber hinaus werden die Werte bzw. Eigentumsrechte auf DLT-Systemen in atomaren Transaktionen transferiert und nicht wie im World Wide Web kopiert; dies verringert das Risiko des Double Spending. Die DLT stellt automatisch sicher, dass ein Wert auf dem Distributed Ledger (bzw. der Blockchain) nur einmal existiert und einem genau identifizierten Besitzer zugeordnet ist. Da auf DLT-Systemen eine zentrale Autorität in der Regel fehlt, sind die Daten auf den dezentral ausgerichteten Nodes gespeichert.[10]

Ferner ist im Rahmen der DLT oft die Rede von «Manipulationssicherheit».[11] Aufgrund der fehlenden zentralen Autorität auf der DLT besteht keine Möglichkeit, die Transaktionshistorie oder die Daten zu manipulieren. Zudem ist es praktisch kaum möglich, die auf den vielen Nodes gespiegelten Daten allesamt zu verlieren.[12]

---

9 Beim Double Spending übermitteln die Angreifer ihrer Gegenpartei, dass die Transaktion bestätigt wurde, und überzeugen gleichzeitig das gesamte Netzwerk, dass eine andere Transaktion zu akzeptieren ist. Dieser Angriff ist nur möglich, wenn nicht alle Nodes denselben Informationsstandard haben; im Grundsatz handelt es sich um ein Problem der Synchronisation von Transaktionen, da Informationen immer eine gewisse, kurze Zeit benötigen, bis sie bei allen Nodes ankommen (*Sayeed/Marco-Gisbert*, 2019, 4 f. m.w.H.; *Rosenfeld*, 2014, 2).

10 *Rutishauser/Kubli/Weber*, 2021, Rz. 4 f.

11 Vgl. zur Manipulationssicherheit auch Kap. II.B.3.a).

12 *Rutishauser/Kubli/Weber*, 2021, Rz. 6.

3. Arten der DLT

Die auf DLT basierenden Systeme lassen sich in permissionless und permissioned DLT-Systeme kategorisieren. Auf permissionless Systemen kann jedermann die Validierung der Blocks vornehmen; die Durchführung und Validierung auf permissioned Systemen ist auf die autorisierten Teilnehmenden beschränkt.[13] Diese Kategorisierung ist insbesondere im Hinblick auf die Sicherheit und Resilienz der Systeme von Bedeutung, weil das Geschehen auf permissioned DLT-Systemen besser kontrollierbar ist.

Neben (bzw. zusammen mit) dieser Abgrenzung gibt es auch die Kategorisierung in private, öffentliche und konsortiale Systeme; diese Unterteilung hängt von der Authentifizierung der Benutzer und von der Führung der Plattform ab.[14]

Auf öffentlichen Systemen fehlt eine Einheit, welche die Leitung des Systems übernimmt, die Transaktionen auf diesen Systemen sind öffentlich und die Nutzer wahren ihre Anonymität; ferner kommt den Teilnehmenden keine privilegierte Entscheidungsmacht zu; Entscheidungen basieren auf dem Konsensmechanismus. Findet eine Unterscheidung zwischen den permissioned/permissionless sowie den öffentlichen und privaten Systemen statt, sind die meisten öffentlichen Systeme gleichzeitig permissionless Systeme, d.h. es besteht für jedermann ein uneingeschränkter Zugriff auf das Netzwerk.[15]

Neben den öffentlichen Systemen existieren private DLT-Systeme; auf privaten Systemen können nur autorisierte Parteien die Transaktionshistorie (im Rahmen von Transaktionen insbesondere auf der Blockchain) einsehen. Zudem ist der Zugang zum System lediglich eingeschränkt möglich und die Teilnehmenden sind grundsätzlich identifizierbar. Es obliegt der kontrollierenden Partei, die Regeln des Konsenses festzulegen; grundsätzlich ist nur einer be-

13 *Ganne*, 2021, 130; *Low*, 2020, 7 f.; *Low/Mik*, 2020, 138 ff.; *Nascimento/Pólvora*, 2019, 14; *Rauchs et al.*, 2018, 24; *Ganne*, 2018, 8; *Hon/Palfreyman/Tegart*, 2016, 12 f.

14 *Deng/Lee*, 2017, 147 wonach die Terminologie nicht einheitlich benutzt wird in der Literatur; *Low/Mik*, 2020, 138; *World Bank Group*, 2017, IV unterscheidet beispielsweise ausdrücklich permissioned und permissionless sowie private und public Blockchains bzw. Distributed Ledgers.

15 *Rutishauser/Kubli/Weber*, 2021, Rz. 20 f.; *Salmon/Myers*, 2019, 1 f.; *Nascimento/Pólvora*, 2019, 14 f.; *Ganne*, 2018, 9 f.

schränkten Anzahl Nodes erlaubt, am Verifikationsprozess teilzunehmen. In dieser Konstellation ist das System nicht nur technologisch, sondern auch organisatorisch über umfassende Vertrags- bzw. Regelwerke geschützt.[16]

Konsortiale Systeme (oft Consortium Distributed Ledgers) sind eine Unterkategorie der privaten Systeme; sie werden von einer Gruppe an Stelle von bloss einer Partei betrieben, welche die Teilnehmenden identifiziert. In diesen Systemen gibt es ebenfalls vorbestimmte Nodes, die am Verifikationsprozess teilnehmen können.[17]

Bei den hier dargestellten Kategorisierungen der DLT handelt es sich nicht um eine abschliessende Liste; es sind insbesondere auch hybride Systeme denkbar.

B. Konzept der DLT

Verschiedene DLT-Ideen beanspruchen für sich teilweise, das Vertrauen in das Finanzsystem zurückzubringen, da sie oft ohne «vertrauensunwürdige» Intermediäre, wie z.B. Banken, funktionieren und als sicher gelten. Nachfolgend sind die wichtigsten Konzepte und technologischen Grundlagen der DLT zu erläutern, um ein grundlegendes Verständnis für die rechtliche Analyse des DLT-Gesetzes zu schaffen.[18]

1. Verteilte Register mit automatischem Protokoll

In den Distributed Ledgers hat – wie erwähnt – nie eine Einzelpartei die Kontrolle über die ganzen Register bzw. sind die Daten nie zentral an einer Stelle gespeichert; vielmehr verteilen sich verschiedene Spiegelungen mit demselben Informationsgehalt auf mehrere Nodes, welche die Rolle der Zentralpartei in «traditionellen» Konstellationen übernehmen.[19] Dieses Konzept stellt sicher, dass kein Single Point of Failure (dt. einzelner Ausfallpunkt) existiert. Die Verbesserung der Sicherheit weist aber auch eine Kehrseite auf, nämlich den Konsensmechanismus: Die Teilnehmenden selbst sind dafür zuständig, mit einem Konsensmechanismus die Datenblöcke zu verifizieren und zu va-

16 *Rutishauser/Kubli/Weber*, 2021, Rz. 20 f.; *Salmon/Myers*, 2019, 1 f.; *Nascimento/Pólvora*, 2019, 14 f.; *Ganne*, 2018, 10; *Kaulartz*, 2016, 475.

17 *Ganne*, 2018, 11; *Rauchs et al.*, 2018, 54.

18 So auch *Schär/Berentsen*, 2020, 31 ff.

19 *Low*, 2020, 7; *Ganne*, 2018, 6.

lidieren;[20] dieser Konsensmechanismus ersetzt das Vertrauen in die Gegenpartei. Bei der Blockchain beispielsweise regelt das Blockchain-Protokoll das Konsensverfahren, d.h. die Aktivität aller Teilnehmenden basiert auf diesem Protokoll, welches Instruktionen für das gesamte Netzwerk enthält. In der Regel ist dieser Code «Open Source», d.h. er ist für alle Teilnehmenden einsehbar und nachvollziehbar.[21]

Wie erwähnt, ist die Blockchain ein (bzw. der wohl bekannteste) Anwendungsfall der Distributed Ledger, welche eine umfassendere Umschreibung der Technologie beinhaltet. Andere Formen der Distributed Ledger sind in der Praxis noch nicht verbreitet, aber es gibt beispielsweise auch die Hashgraphs.[22]

2. Fehlende Intermediäre und dezentrale Transaktionen

Entsprechend der Umschreibung als «Internet der Werte» betrifft eine Hauptfunktion der DLT (und im Kontext der Transaktionen bei der Blockchain) den Aspekt, welcher Wert von einer Partei auf eine andere Partei übertragen wurde (wieviel und was). Die Daten jeder Transaktion bzw. jedes Bündels von Transaktionen lassen sich als Block auf der Blockchain repräsentieren. Jeder Block hat einen Header, der alle erforderlichen Informationen enthält, um einen Block einordnen und validieren zu können, und einen Body, der die zu registrierende Transaktion beschreibt. Da jeder Block in der Kette auf dem vorherigen Block aufbaut, ist es möglich, die ganze Kette zurückzuverfolgen; ein neu geschaffener Block enthält den Hash des vorangehenden Blocks.[23]

Die Idee der Unveränderbarkeit der Blockchain lässt sich auf den Umstand zurückführen, dass bei einem Angriffsversuch, der einen Block abändern will, sowohl der Hash dieses Blocks als auch jene Hashs in den darauffolgenden Blocks invalide sind. Da zudem die Transaktionen atomar sind, also die Buchungen und Berechnungen innerhalb der Transaktionsklammer stattfinden, können

20 *Weber*, 2021a, Rz. 11; *Low*, 2020, 7; *Ganne*, 2018, 5 ff.; *Maull et al.*, 2017, 483 f.

21 *Rutishauser/Kubli/Weber*, 2021, Rz. 15.

22 Beim Hashgraph wird jeder Container von Transaktionen in das Ledger aufgenommen; im Gegensatz zur Blockchain, die einen Fork erlaubt, kann kein Container verworfen werden. Alle Zweige bleiben immer bestehen und bilden ein Ganzes (vgl. *Baird/Harmon/Madsen*, 2020, 9 f. mit bildlicher Gegenüberstellung der Blockchain und Hashgraphs); vgl. ferner *Rutishauser/Kubli/Weber*, 2021, Rz. 14.

23 *Rutishauser/Kubli/Weber*, 2021, Rz. 16.

die Transaktionen nur insgesamt ausgeführt oder insgesamt nicht ausgeführt werden; daraus folgt, dass sich grundsätzlich Settlement- oder Rekonziliationsprozesse erübrigen.[24]

Trotz der fehlenden Intermediäre erlaubt das Konzept der DLT, die Transaktionen zu validieren. Gestützt auf einen besonderen Konsensmechanismus[25] im Smart Contract[26] lassen sich die Transaktionen ausführen. Dabei ist in der Regel eine Validierung aller Nodes notwendig; die genauen Regelungen sind im Smart Contract festzuhalten.[27]

3. Konsensmechanismen

a) Grundlagen

Auf den Distributed Ledgers gibt es grundsätzlich zwei Arten von Nutzern, und zwar jene, die nur Transaktionen registrieren, und jene, die durch den Betrieb von Nodes diejenige Rechenleistung zur Verfügung stellen, welche die Transaktion validiert. Die Teilnehmenden der zweiten Gruppe sind – gestützt auf einen spezifischen Konsensmechanismus – für die Findung des Konsenses zuständig; in der DLT ersetzt dieser Konsensmechanismus das Vertrauen in die Gegenpartei. Die Konsensmechanismen sind – anders als der Name andeutet – keine demokratischen Meinungsübereinstimmungsmechanismen, sondern vollständig automatisierte, deterministische und durch einen Algorithmus gesteuerte Validierungsprozesse. Die Validierung hängt somit von der Erfüllung gewisser technologischer Bedingungen ab; im Prinzip kann ein Node bzw. die dahinterstehende Person nicht selbst entscheiden, ob sie eine Transaktion, welche alle Validierungskriterien erfüllt, ablehnen oder eine Transaktion, welche die Validierungskriterien nicht erfüllt, annehmen will.[28]

Da die öffentlichen Distributed Ledgers (und im Kontext der Transaktionen insbesondere die öffentlichen Blockchains) jederzeit allen Teilnehmenden (und die privaten einer vordefinierten Gruppe von Teilnehmenden) zur Verfügung stehen, sind alle Transaktionen transparent und später einsehbar. Dies kann aber problematisch sein, wenn gewisse Informationen nicht öffentlich verfügbar gemacht werden wollen bzw. wenn sie im Nachhinein aufgrund von

24 *Rutishauser/Kubli/Weber*, 2021, Rz. 17 f.

25 Vgl. zum Konsensmechanismus Kap. II.B.3.

26 Vgl. zum Smart Contract Kap. II.B.5.

27 Vgl. im Detail *Schär/Berentsen*, 2020, 36 ff.; *Rutishauser/Kubli/Weber*, 2021, Rz. 19.

28 *Low/Mik*, 2020, 140 f.

Fehlern abzuändern sind. Eine mögliche Lösung hierfür kann die Speicherung auf einer Off-Chain (oder auf einer Side-Chain) sein. Eine Side-Chain ist eine sekundäre Blockchain, die mit der primären Blockchain verbunden ist. Die Side-Chains können eigene Konsensprotokolle besitzen, die sich vom Konsensprotokoll der primären Blockchain unterscheiden; sie werden u.a. zur Verbesserung des Datenschutzes und der Sicherheit der primären Blockchain eingesetzt. Mittels Side-Chains können die Daten mit einer Hash-Referenz (engl. hash reference) an die Blockchain gebunden werden, um den Zugang zu diesen sensiblen Daten nur bestimmten, autorisierten Parteien zu erlauben.[29]

Aufgrund dieses Konsensmechanismus (und der generellen Funktionsweise der Distributed Ledgers) wird die DLT und die Blockchain regelmässig als manipulationssicher (engl. temper resistence) angesehen. Eine wichtige Eigenschaft besteht darin, dass die Änderung und Löschung einer bereits aufgezeichneten Transaktion kaum möglich ist, da jeder angefügte Block in der Blockchain einen Zeitstempel enthält und jede Änderung für die Teilnehmenden einsehbar ist. Die Manipulationssicherheit kann jedoch nicht die Authentizität der gespeicherten Informationen gewährleisten. Ferner sind die DLT-Systeme nicht unveränderlich, sondern bloss schwer veränderbar; gestützt auf den zugrundeliegenden Konsensmechanismus eines Systems können die Teilnehmenden u.a. über eine Änderung der Blockchain abstimmen.[30]

In der Praxis haben sich insbesondere folgende zwei Methoden als Konsensmechanismus etabliert:[31]

b) Proof of Work

Bei der Proof of Work-Methode versuchen die Teilnehmenden, eine komplexe Proof of Work-Instanz (eine komplexe Berechnung)[32] zu lösen. Die Proof of Work baut auf der Asymmetrie der Berechnung und Verifizierung auf, denn für die Berechnung sind immense Rechenleistungen erforderlich, während die Verifikation der Lösung einfach ist. Dabei bekommt die erste Partei, welche die Lösung findet, eine Belohnung und die übrigen Teilnehmenden können diese Lösung einfach nachprüfen. Dieser geschilderte Verifizierungsprozess wird

29 Vgl. *Singha et al.*, 2020, 1 ff.; vgl. ferner *Nascimento/Pólvora*, 2019, 17 f.; *Maull et al.*, 2017, 483 f.

30 *Walch*, 2017, 739 f.; vgl. auch *Nascimento/Pólvora*, 2019, 17; EZB, 2017, 19.

31 *Rutishauser/Kubli/Weber*, 2021, Rz. 22 ff.; vgl. *Schär/Berentsen*, 2020, 139 ff.

32 Genau genommen handelt es sich dabei nicht um eine übliche Mathematik-Rechnung, sondern um ein komplexes Verfahren, vgl. hierfür im Detail *Gervais et al.*, 2016, 4 f.

als Mining bezeichnet, da sich mit der Verifizierung ein neuer Block in die Blockchain einreiht. Die Proof of Work ist eine etablierte Methode zur Konsensfindung, die beispielsweise auch beim Bitcoin-Netzwerk zur Anwendung gelangt.[33] Sie weist aber einige Nachteile auf: Es besteht die theoretische Möglichkeit, dass Betreiber von Rechenfarmen mit hoher Rechenleistung den Verifizierungsprozess zentralisieren könnten.[34] Zudem ist die Proof of Work sehr energieintensiv; mit dem «Ethereum Merge» (Umstellung auf Proof of Stake) sollen schätzungsweise 99% des Energieverbrauchs gespart werden.[35]

c) Proof of Stake

Beim Proof of Stake erfolgt die Validierung nicht über die Rechenleistung der Teilnehmenden, sondern über hinterlegte Kryptowährungen. Beim Proof of Stake ist zwischen den Validierern, die ihr Vermögen gesperrt haben (engl. staked coins), und jenen, die bloss die Kryptowährung des entsprechenden Systems besitzen (z.B. die Währung Bitcoin bei Bitcoin oder die Währung Ether bei Ethereum), zu unterscheiden. Diese letzte Gruppe kann auch die Qualifikation eines Validierers erhalten, wenn die Mitglieder mittels einer speziellen Transaktion ihre Kryptowährung in einem Depot sperren (engl. staking). Dabei schlagen die Validierer durch eine gewichtete Zufallsauswahl, deren Ermittlung durch die Teilnahmedauer und/oder die prozentuale Relation zu den hinterlegten Kryptowährungen erfolgt, den potenziell nächsten, validen Block vor und stimmen über dessen Gültigkeit ab. Die Stimmkraft der Validierer hängt dabei von der Grösse ihres hinterlegten Depots ab.[36]

Das Staking wird ergänzt durch ein Slashing; weil das DLT-System effizient funktionieren muss, braucht es eine stabile und sichere Leistung der Validierer. Das Slashing dient der Bestrafung unlauteren bzw. böswilligen Verhaltens der Validierer. Einerseits sind die Validierer bei diesem Prozess dem Risiko ausgesetzt, ihr gesamtes Depot bzw. Teile der hinterlegten Kryptowährungen zu verlieren;[37] andererseits erhalten die Validierer eine kleine Belohnung pro-

33 *Nakamoto*, 2008, 3.

34 *Rutishauser/Kubli/Weber*, 2021, Rz. 22 ff.; *Chentouf/Bouchkaren*, 2021, 74.

35 Vgl. weiterführend zum «Ethereum Merge» Kap. II.B.3.c).

36 *Antonopoulos/Wood*, 2019, 321.

37 *Rutishauser/Kubli/Weber*, 2021, Rz. 27; *Chentouf/Bouchkaren*, 2021, 74; *Bitcoinsuisse*, 2020, 1 f.

portional zu ihrem hinterlegten Depot. Dieser Mechanismus mit Belohnung und Bestrafung zwingt die Validierer dazu, ehrlich zu handeln und das Konsensprotokoll zu verfolgen.[38]

Mitte September 2022 ist es zu einer Umstellung des Konsensmechanismus bei Ethereum gekommen; nach dem «Ethereum Merge» läuft die Validierung über die Proof of Stake-Methode und nicht mehr über den Proof of Work. Mit diesem Merge strebt Ethereum eine schnellere Durchführung der Transaktionen auf der Blockchain sowie eine erhebliche Senkung des Energieverbrauchs (schätzungsweise um 99%) an.[39]

4. Wallets

a) Grundlagen

Damit die Nutzerinnen und Nutzer die DLT-Systeme sinnvoll nutzen können, brauchen sie auch eine Möglichkeit, ihre Kryptowerte aufzubewahren und auf diese zurückzugreifen. Dies geschieht in der Regel mittels sog. Wallets (dt. Geldbörse).[40]

Die Wallets lassen sich in «Cold Wallets» und «Hot Wallets» unterteilen.[41] In der Praxis ist die Verwendung der Hot Wallets verbreitet, da sie eine hohe Nutzerfreundlichkeit aufweisen; die Hot Wallets sind eine Software, welche auf einem Computer bzw. einem Smartphone aufrufbar ist und eine direkte Verbindung zum Internet hat. Der Nachteil der Hot Wallets besteht darin, dass sie das Angriffsziel von Cyberattacken sein können, da sie ein einfaches Ziel darstellen. Aus diesem Grund ist es empfehlenswert, grössere Mengen von Kryptowerten in Cold Wallets aufzubewahren. Die Cold Wallets sind nicht direkt

---

38 *Antonopoulos/Wood*, 2019, 321.

39 *Mathias Born*, Ethereum senkt Stromverbrauch: Wie Bitcoin, nur bio, Tages-Anzeiger vom 15.09.2022, aufrufbar unter <https://www.tagesanzeiger.ch/die-zweitgroesste-kryptowaehrung-wird-oekologischer-652418632805>; *Ruth Fulterer*, Ethereum löst auf einen Schlag sein Energieproblem. Das geht nicht ohne Risiko. Die sieben wichtigsten Fragen, NZZ vom 29.08.2022, aufrufbar unter <https://www.nzz.ch/technologie/der-merge-bei-ethereum-7-fragen-zum-gruenen-umbau-der-blockchain-ld.1695122>.

40 *Rutishauser/Kubli/Weber*, 2021, Rz. 28.

41 *Urien*, 2021, 49.

mit dem Internet bzw. mit sonst einem Netzwerk verbunden und befinden sich in der Regel auf einem Hardware-Gerät (z.B. externe Festplatte oder USB-Stick) oder die Zugangsdaten sind auf einem Stück Papier festgehalten.[42]

Die Wallets bestehen grundsätzlich aus zwei Teilen: Einerseits aus einem Satz privater Schlüssel,[43] welche die Transaktion signieren, andererseits aus einer Reihe von erforderlichen Parametern, welche die Transaktionen generieren. Daraus folgt, dass auch die Private Keys in der Regel in der Wallet aufbewahrt werden.[44]

b) Sicherung der Private Keys

Für die Sicherung der Private Keys stehen verschiedene Möglichkeiten zur Verfügung, welche Ähnlichkeiten zu den Hot und Cold Wallets aufweisen. Nachfolgend sind zwei Methoden für das allgemeine Verständnis näher zu erläutern:

aa) Key in Local Storage

Bei dieser Methode wird der Private Key lokal gespeichert sowie ver- und entschlüsselt. Derjenige, der das DLT-System benutzt, ist dabei in der Lage, bei jeder neuen Transaktion auf den Schlüssel zuzugreifen und die Transaktion an das Netzwerk zu übertragen.

Der Vorteil dieser Variante besteht in der Entlastung der Teilnehmenden, da sie in der Regel – nach Abspeicherung des Private Key – nichts Weiteres vornehmen müssen, weil die Nutzerinnen und Nutzer selbst die erforderlichen Schritte einleiten; zudem ist es möglich, eine sehr grosse Anzahl an Schlüsseln lokal zu speichern, da die Private Keys nur wenig Datenvolumen erfordern.[45]

Lokal gespeicherte private Schlüssel weisen aber auch Nachteile auf, da jedermann mit Zugriff auf den Ordner mit den Private Keys die Schlüssel lesen kann. Es ist insbesondere zu beachten, dass die Angreifenden mit herkömmlichen Methoden die Schlüssel zu stehlen versuchen; denkbare Konstellationen für einen Diebstahl sind die unfreiwillige Freigabe der entsprechenden Ordner (z.B. auf einem freigegebenen Netzlaufwerk) oder auch der physische Dieb-

42 *Das/Faust/Loss*, 2019, 651.

43 Hernach grundsätzlich in der üblichen Terminologie «Private Key».

44 *Urien*, 2021, 49; *Jian/Ran/Liyan*, 2021, 47; *Tschorsch/Scheuermann*, 2016, 2088 und 2092 f.

45 *Eskandari/Barrera/Stobert/Clark*, 2018, 2 f.; vgl. ferner *Pala/Alamb/Thakura/Singh*, 2021, 78.

stahl eines Notebooks bzw. Smartphones. Ferner ist zu bedenken, dass bei der lokalen Speicherung insbesondere der menschliche Fehlerfaktor entscheidend ist und nicht die Sicherheit des DLT-Systems an sich, da nicht das DLT-System unmittelbares Angriffsziel ist; diese Fehlerquelle lässt sich mittels Verschlüsselung des Private Key mit einem Passwort minimieren, jedoch besteht die Möglichkeit, mit der Installation von Malware Logging-Modulen den Nutzen des Passworts zu beseitigen.[46]

bb) Offline Storage of Keys

Eine andere Methode ist die offline Speicherung der Schlüssel (z.B. auf einer externen Festplatte oder [handschriftlich] auf Papier); dadurch lässt sich der unberechtigte, digitale Zugriff auf den Schlüssel auf die kurze Spanne der Verwendung des Speichergeräts begrenzen. Externe Festplatten bleiben aber auch bei dieser Herangehensweise potenzielle Angriffsziele von Malware, da diese nur durch Anschluss an einen Computer funktionieren. Interessant ist ebenso die Speicherung des Schlüssels mittels schriftlicher «Speicherung» der entsprechenden Zeichenfolge auf Papier.

Obwohl (bzw. weil) die offline Speicherung im weitesten Sinne mit dem Mitführen von Bargeld verglichen werden kann, ist auch hier der menschlichen Fehlerfaktor entscheidend, da der Mensch das Speichergerät verlieren bzw. an einen mit Malware infizierten Computer anschliessen kann.[47]

5. Smart Contracts

Das Konzept der Smart Contracts ist nicht erst mit den neusten Entwicklungen im DLT- und Blockchain-Bereich aufgekommen. Als «Erfinder» der Smart Contracts gilt *Szabo*, der den Smart Contract als «*a computerized transaction protocol that executes the terms of a contract*» umschreibt.[48] In seinem Beispiel nennt *Szabo* den Anwendungsfall der Münz- bzw. Verkaufsautomaten: Wenn die richtige Münze eingeworfen wird, lässt die Maschine das gewünschte Produkt raus; wenn keine Produkte mehr vorhanden sind oder die falsche Münze

46 *Eskandari/Barrera/Stobert/Clark*, 2018, 2.

47 *Eskandari/Barrera/Stobert/Clark*, 2018, 2 f.; vgl. ferner *Pala/Alamb/Thakura/Singh*, 2021, 78.

48 *Szabo*, 1994.

eingeworfen wurde, lässt die Maschine die Münze wieder raus. Charakteristisch hierfür ist, dass die Transaktion während der Durchführung nicht gestoppt werden kann.[49]

Szabo hält aber auch fest, dass die Anwendungsfälle sich nicht auf dieses Beispiel beschränken, sondern in allen von digitalen Mitteln kontrollierten Verhältnissen vorstellbar sind. Smart Contracts können folglich zwar gänzlich ohne DLT bestehen, jedoch erlaubt die DLT eine angemessenere und effizientere Anwendung der Smart Contracts auf einem weltweit dezentralen Netzwerk.[50]

Im Gegensatz zum Beispiel mit dem Münz- bzw. Verkaufsautomaten lässt sich der Smart Contract auf der DLT ohne die physische Anwesenheit der Parteien durchführen.[51] Es handelt sich dabei um eine Art Anwendung auf der Blockchain, die parallel durch verschiedene Validierende ausgeführt wird. Sie basiert auf vorbestimmten Regeln (grundsätzlich auf Wenn-Dann-Regeln); ist der Smart Contract auf der Blockchain gespeichert und tritt ein vordefiniertes Szenario ein, dann wird der Vertrag automatisch – gemäss den vorbestimmten Folgen – vollzogen.[52] In diesem Sinne braucht es für den Vollzug des Smart Contract nicht zwingend einen «üblichen» Konsens im Rechtssinne, sondern bloss den Eintritt des vordefinierten Ereignisses (dieses Ereignis kann einen Konsens voraussetzen, muss es aber nicht).[53] Insofern sind Smart Contracts auch nicht Verträge im rechtlichen Sinne, sondern Programme, die Prozessabläufe auf einer Blockchain automatisieren und die korrekte Ausführung von vertraglichen Beziehungen sicherstellen.[54]

Gestützt auf diesen Aufbau wird der Smart Contract immer wie vordefiniert ausgeführt und alle Teilnehmenden können die getätigten Änderungen durch den Smart Contract jederzeit verifizieren, d.h. bei korrekter Implementierung sind die Smart Contracts transparent und vermögen das Risiko einer Manipulation bzw. eines willkürlichen Eingriffs einzuschränken. Darüber hinaus sind die Smart Contracts sehr flexibel und vielfältig einsetzbar, da sie auch Krypto-Werte speichern und dadurch die Rolle eines Verwahrers einnehmen können.

---

49 *Szabo*, 1996.

50 *Ibid.*

51 *Madir*, 2019, Rz. 7.04; *Szabo*, 1996.

52 Vgl. *Weber*, 2017c, Rz. 3 f.

53 *Schär*, 2021, 154; *Wang et al.*, 2018, 110.

54 *Rutishauser/Kubli/Weber*, 2021, Rz. 32; *Schär/Hübner*, 2020, 305.

Dabei lässt sich der Smart Contract so individualisieren, dass beispielsweise festgehalten wird, an welche Person, zu welchem Zeitpunkt und auf welche Art die Assets freigegeben werden können.[55]

6. Oracles

Die Smart Contracts benötigen in der Regel einen «Zugang» zu Informationen ausserhalb der Blockchain (engl. off-chain information), um beschliessen zu können, wann die Ausführung erfolgen soll, weil das DLT-System bzw. konkret die Blockchain selbst nicht «sieht» bzw. wahrnimmt, was off-chain geschieht. Weil das DLT-System bzw. die Blockchain aber auf einem Konsensmechanismus basiert und die Nodes solche Informationen als «nicht vertrauenswürdig» qualifizieren würden, können solche Daten nicht über Transaktionsdaten vermittelt werden. Aus diesem Grund braucht es in allen Fällen, die von einem off-chain Ereignis abhängen, ein Oracle, der den Smart Contract «freigibt».[56]

Oracles sind zentralisierte, vertrauenswürdige «Drittparteien», welche die Verbindung zwischen der Blockchain und der «realen Welt» bzw. der off-chain Welt herzustellen vermögen; sie können somit Daten zwischen der Blockchain und der Aussenwelt transferieren.[57] Genau betrachtet, führen die Oracles also nicht Informationen in die Blockchain ein, sondern sie sammeln und speichern Informationen der realen Welt. Sobald ein Smart Contract diese Daten benötigt, ruft der Code die erforderlichen Informationen vom Oracle ab.[58]

Da aber die Oracles als zentralisierter Single Point of Failure anzusehen sind, führen sie das vorgenannte Sicherheitsproblem wieder ein[59] und verursachen folglich Cybersicherheitsbedenken.[60] *Curran* definiert die Oracle-Problematik als «*the security, authenticity, and trust conflict between third-party oracles and the trustless execution of smart contracts*».[61]

---

55 *Schär*, 2021, 154.

56 *Low/Mik*, 2020, 172; *Caldarelli*, 2020, 4.

57 *Yuxi/Fragkos/Tsiropoulou/Veneris*, 2020, 128; *Mühlberger et al.*, 2020, 36.

58 *Caldarelli*, 2020, 4.

59 Vgl. zum Vorteil der Blockchain-Technologie, wonach gestützt auf das eigentliche Konzept der Blockchain kein Single Point of Failure existiert Kap. II.B.1.

60 Es gibt bereits erste Ansätze von dezentralisierten Oracles, die auf bestimmten Abstimmungsmechanismen basieren, aber noch nicht ausgereift sind, vgl. z.B. *Yuxi/Fragkos/Tsiropoulou/Veneris*, 2020, 128 f.; *Caldarelli*, 2020, 5.

61 *Curran*, 2018.

Da die Oracles mit «nicht-deterministischen» Daten funktionieren, ist die Vertrauenswürdigkeit von grösster Bedeutung bei der Auswahl des Oracle; jedoch wirkt die Einführung eines Oracle dem Prinzip der Peer-to-Peer-Interaktion auf DLT-Systemen bzw. auf der Blockchain, die unabhängig von bestimmten Vertrauenselementen funktioniert, entgegen. Gleichzeitig kann die Implementierung der Oracles das Vertrauen der Nutzer in die DLT-Systeme gefährden.[62]

Zudem können Systeme, die auf Oracles aufbauen, aus weiteren Gründen scheitern: Selbst wenn das Oracle vertrauenswürdig und nicht gefährdet ist, besteht die Möglichkeit, dass die Daten des Oracle modifiziert wurden und deshalb trotz seiner Vertrauenswürdigkeit der Smart Contract unwahre Daten zur Verfügung gestellt erhält.[63]

7. Token und Tokenisierung

Wie bereits dargestellt, erlaubt die DLT, die Digital Assets (dt. digitale Vermögen) ohne Intermediäre zu besitzen und zu transferieren; diese Assets, die sich auf DLT-Systemen darstellen lassen, können aber bloss Vermögenswerte sein, die als Teil des zugrundeliegenden Protokolls erstellt wurden. Will man auf Distributed Ledgers externe Assets verfolgen und handeln, müssen diese Vermögenswerte tokenisiert werden. Somit gilt der Token im Kontext der Distributed Ledgers als digitale Repräsentation eines Gutes und kann wie Assets, die Teil des zugrundeliegenden Protokolls sind, gehandelt werden.[64] Ein Token lässt sich somit auch als digitalisierter Schuldschein für ein zugrundeliegendes Recht definieren; dieser Schuldschein existiert im übertragenen Sinne als individualisierter Eintrag in einer Datenbank.[65]

Grundsätzlich lässt sich allen Wertgegenständen ein digitales Äquivalent zuordnen. Dies erlaubt die «Zerstückelung» der digitalen Repräsentation; in der «realen» Welt kann man ein analoges Gut in der Regel nicht so einfach in verschiedene Teile stückeln. Dieser Prozess der digitalen Repräsentation und der «Zerstückelung» nennt sich Tokenisierung.[66]

In der Schweiz hat die FINMA die Token im Februar 2018 in drei Kategorien gegliedert, und zwar in Zahlungs-Token, Nutzungs-Token sowie Anlage-Token:[67]

62 *Caldarelli*, 2020, 5.

63 *Antonopoulos/Wood*, 2019, 265 f.

64 *Roth/Schär/Schöpfer*, 2021, 332; *Varmaz/Varmaz/Günther/Poddig*, 2021, Rz. 35.

65 *Varmaz/Varmaz/Günther/Poddig*, 2021, Rz. 35.

66 *Rutishauser/Kubli/Weber*, 2021, Rz. 33.

67 FINMA, 2018a, 3; zur Klassifizierung der Token im Detail, vgl. *Weber/Baisch*, 2021, 684 ff.

- Zahlungs-Token sind Token, die tatsächlich oder nach Absicht der Organisatoren als Zahlungsmittel verwendet und akzeptiert werden sollen; Zahlungs-Token können auch der Geld- oder Wertübertragung dienen.
- Demgegenüber gewähren Nutzungs-Token den Zugang zur digitalen Nutzung bzw. zu einer Dienstleistung, welche die Betreibenden der DLT-Systeme auf den Distributed Ledgers anbieten.
- Anlage-Token repräsentieren Vermögenswerte; Anlage-Token können schuldrechtliche Forderungen gegenüber den Emittenten oder auch ein Mitgliedschaftsrecht im gesellschaftsrechtlichen Sinne darstellen. Diese Token stehen somit – je nach wirtschaftlicher Funktion – für eine Aktie, eine Obligation oder für ein derivatives Finanzinstrument; auch Token, die physische Wertgegenstände auf DLT-Systemen handelbar machen, sind als Anlage-Token zu qualifizieren.

Diese Klassifizierung stellt keine abschliessende Gruppenbildung dar und die einzelnen Kategorien schliessen sich nicht aus. Es ist insbesondere denkbar, dass hybride Token existieren, also dass z.B. Anlage- und Nutzungs-Token zusätzlich in die Kategorie von Zahlungs-Token fallen. In diesen Fällen lässt sich der Token gleichzeitig als Effekte und Zahlungsmittel qualifizieren.[68]

C. Anwendungsbereich der DLT

Eine grundsätzliche Frage im DLT-Kontext besteht darin, wie die dezentrale Organisation der DLT in einem zentral regulierten Umfeld wie dem Finanzmarktrecht umgesetzt werden kann. Sinn der Technologie ist gerade, eine zentrale Autorität zu vermeiden und in einem dezentralen Netzwerk zu funktionieren. Trotz dieser Schwierigkeit gibt es einige Anwendungsfälle. Aus diesem Grund ist zunächst der Einsatz von DLT-Lösungen zu diskutieren (1.), bevor auf die Eigenschaften dieser Lösungen eingegangen wird (2.). Schliesslich ist auch die wirtschaftliche Bedeutung der DLT darzulegen (3.).

1. Einsatz der DLT

Die DLT bringt nur in bestimmten, definierten Situationen einen tatsächlichen Mehrwert. Im Falle einer Implementierung der DLT in ein System, das nicht die Vorteile dieser Technologie ausnutzen kann, ergeben sich verzichtbare Pro-

[68] FINMA, 2018a, 3.

bleme und die Komplexität des Gesamtsystems erhöht sich unnötig. Überblicksweise lassen sich folgende, generelle Kriterien für den Einsatz der DLT nennen:[69]

1. Das System kann seine Vorteile durch den dezentralen Aufbau ausnutzen; dabei laufen die Transaktionen zwischen den einzelnen Teilnehmenden ab und nicht über eine zentrale Stelle, die einem Ausfallrisiko ausgesetzt ist.
2. Die Automatisierung der Abläufe durch Smart Contracts bringt eine Effizienzsteigerung, denn die Transaktionen sind auditierbar und werden – gestützt auf im Code festgelegten Bedingungen – automatisch ausgeführt.
3. Bei digitalisierten Vermögensgegenständen ist ein effizienter Eigentümerwechsel anzustreben.
4. Das Ökosystem hat mehrere Parteien, die durch unterschiedliche Anreize getrieben sind.
5. Das Ökosystem hat einen wirtschaftlichen Vorteil, wenn es an den Transaktionen teilnimmt.
6. Das System erfordert eine «wahre Datenquelle», über die sich die Teilnehmenden einigen und worauf sie vertrauen können.

In diesem Zusammenhang ist es wichtig, neben dem technologischen Nutzen auch die funktionelle und rechtliche Umsetzung potenzieller Systeme auszuwerten. Deshalb sind die Kosten im Rahmen der Forschung und Entwicklung, der Implementation und der Aufrechterhaltung sowie die rechtliche Regulierungslandschaft mit angeschnittenen Rechtsbereichen von Bedeutung.[70]

2. Eigenschaften der DLT-Lösungen

Die Umsetzung der DLT bietet insbesondere in folgenden Bereichen bzw. Szenarien Vorteile:[71]

1. Die auf den Distributed Ledgers gespeicherten Daten sind unveränderlich bzw. sehr schwer veränderbar.[72] Dies lässt sich auf die fehlende, zentrale Autorität zurückführen; es gibt also keine zentrale Stelle mit Macht, wel-

69 *Rutishauser/Kubli/Weber*, 2021, Rz. 36 f.

70 Vgl. ferner für eine ähnliche Überlegung im Rahmen der Implementierung von Blockchain im öffentlichen Dienst *Urbach et al.*, 2018, 3 f.

71 Vgl. teils auch *Rutishauser/Kubli/Weber*, 2021, Rz. 37.

72 Vgl. zur (Un-)Veränderbarkeit der Daten auf der Blockchain Kap. II.B.3.a).

che in der Lage wäre, bereits bestätigte Daten auf den Distributed Ledgers nachträglich abzuändern. Jeder angefügte Block besitzt einen Zeitstempel und Änderungen sind für die Teilnehmenden ersichtlich. Dies verstärkt das Vertrauen in das System, jedoch gewährleistet die DLT *nicht* die Authentizität der gespeicherten Informationen.

2. Die kryptografischen Methoden ermöglichen eine sichere und unumkehrbare Übertragung von digitalisierten Vermögenswerten.[73]
3. Mit den programmierbaren Smart Contracts lassen sich automatisierte Transaktionen durchführen, die gestützt auf vordefinierte Szenarien erfolgen; dies erlaubt eine gewisse (Planungs-)Sicherheit, da keine zufälligen, sondern nur vorbestimmte Transaktionen möglich sind.

3. Wirtschaftliche Bedeutung der DLT

Der DLT-Bereich verdient nicht nur aufgrund der technologischen Entwicklungen, sondern auch wegen der wirtschaftlichen Bedeutung Aufmerksamkeit. Mit der Blockchain bzw. der DLT allgemein ist es möglich, programmierbare Zahlungen zu tätigen. Dabei handelt es sich um Zahlungen, die gestützt auf vorab festgelegte Bedingungen getätigt werden; solche Zahlungen sind entfernt mit den Daueraufträgen vergleichbar, die an einem vorab bestimmten Kalendertag auszuführen sind. In einem dezentralen Peer-to-Peer Netzwerk ist es auch möglich, komplexere Geschäftsprozesse mit Smart Contracts zu steuern.[74]

Der wirtschaftliche Aufschwung der DLT lässt sich jedoch nicht mit einzelnen, potenziellen Anwendungsfällen begründen; er hängt vielmehr vom Gesamtkonzept der DLT ab; nachfolgend wird auf einige wichtige Punkte hingewiesen.

a) Stabilität durch schwer veränderbare Daten

Von grundlegender Bedeutung ist die schwere Veränderbarkeit der Daten in allen DLT-Systemen, insbesondere der Blockchain. Dies erlaubt beispielsweise eine digitale Verwaltung von Identitäten oder die Durchführung von Wahlen auf Distributed Ledgers, ohne auf dieselben Manipulationsgefahren zu stossen, wie sie bei zentralisierten IT-Systemen existieren. Die DLT ermöglicht

---

73 Vgl. jedoch für potenzielle Lösungen der On-Chain Arbitration auf DLT-Handelsplattformen, die bei allfälligen Streitigkeiten im Rahmen von Übertragungen digitaler Vermögenswerte entstehen können, *Weber/Yildiz*, 2021, Rz. 38 ff.

74 *Diehl*, 2021, Rz. 21.

ferner die Speicherung von (bestimmten) Dokumenten auf den Distributed Ledgers selbst, sodass eine berechtigte Gegenpartei bei Bedarf auf die jeweiligen Informationen bzw. Daten zugreifen kann, und zwar jeweils bloss auf die relevanten Aspekte der Daten und nicht das gesamte Dokument. Die Gegenpartei erhält in diesem Prozess nur die tatsächlich relevanten Informationen für ihre Transaktion, während die Privatsphäre bzw. die nicht erforderlichen Daten weiterhin geschützt bleiben.[75]

b) Kryptowährungen

Obwohl sich die Kryptowährungen als wertinstabil erwiesen haben, sind sie als Pioniere des DLT-Schauplatzes anzusehen. Sie haben dazu beigetragen, dass die Technologie Mainstream-Bekanntheit erlangt und so die Interessen grosser Massen – Investoren, Technologieinteressierte und sogar Staaten[76] – geweckt hat.

Die Volatilität der Währungen schränkt zurzeit noch eine flächendeckende Anwendung der Kryptowährungen ein. Die Wertschwankungen können durch die Kopplung der Kryptowährung an physische Güter bzw. weltweit anerkannte Währungen reduziert werden (Stablecoins).[77] Darüber hinaus lassen sich die Kryptowährungen gegenwärtig in der Regel anonymisiert oder pseudonymisiert verwenden und es fehlt noch an einer klaren Governance. Obwohl diese Punkte nicht für eine weitverbreitete Adaptation der Kryptowährungen sprechen, ist für die Zukunft vorstellbar, die Algorithmen und Transaktionsformen entsprechend abzuändern und so legale Währungsmittel auch in anderen Ländern einzuführen.[78]

---

75 *Rutishauser/Kubli/Weber*, 2021, Rz. 43.

76 Im Jahre 2021 hat beispielsweise El Salvador Bitcoin als gesetzliches Zahlungsmittel akzeptiert, vgl. *Thomas Milz*, Bitcoin in El Salvador: Grosser Bluff oder cooles Zukunftsprojekt?, NZZ vom 22.11.2021, aufrufbar unter <https://www.nzz.ch/finanzen/bitcoin-el-salvador-8000-z-ld.1653805>. Im Jahre 2022 hat die Zentralafrikanische Republik als zweites Land offiziell die Kryptowährung eingeführt, vgl. *Samuel Misteli*, Eines der ärmsten Länder Afrikas führt Bitcoin als offizielle Währung ein. Weshalb, ist ein Rätsel, NZZ vom 07.05.2022, aufrufbar unter <https://www.nzz.ch/wirtschaft/bitcoin-in-zentralafrika-offizielle-waehrung-aber-weshalb-ld.1682821>.

77 Auch über die Stabilität der Stablecoins lässt sich streiten, vgl. u.a. *Helmut Dietl*, Wie stabil sind Stablecoins? Cash vom 29.05.2022, aufrufbar unter <https://www.cash.ch/kolumne/kryptowaehrungen-wie-stabil-sind-stablecoins-1966656>; vgl. ferner *Zellweger-Gutknecht/Weber*, 2022, G 23 ff. m.w.V.

78 Zu den Ansätzen für die Regulierung von Kryptowährungen, vgl. *Zellweger-Gutknecht/Weber*, 2022, G 20 ff.; *Rutishauser/Kubli/Weber*, 2021, Rz. 43; *Diehl*, 2021, Rz. 28.

c) Programmierbares Geld

Mit der DLT haben sich weitere Anwendungsfälle des programmierbaren Geldes entwickelt. Diese Fälle basieren auf einem Vertrag zwischen den involvierten Parteien, der mit einer automatisierten Abwicklung programmiert ist; die Abwicklung lässt sich über eingehende Signale steuern. Tritt die im Voraus definierte Bedingung ein (z.B. Eingang eines bestimmten Signals), wickelt sich der Smart Contract ohne weitere Eingriffe ab.[79]

Anwendungsbeispiele hierfür sind Machine-to-Machine-Zahlungen, bei denen Maschinen auf Rechnung der Besitzer Zahlungen untereinander tätigen. Somit könnte ein selbstfahrendes Auto in Zukunft an der Ladestation für Elektrofahrzeuge selbstständig Elektrizität beziehen und in digitaler Währung den entsprechenden Preis bezahlen. Auch denkbar ist die automatisierte Bezahlung eines Flugzeuges oder Zuges für den Aufenthalt am Flughafen bzw. an einem Bahnhof.[80] Ferner ist an einen Einsatz der Blockchain in den Finanzmärkten, insbesondere an den Handelsplätzen, zu denken.[81]

d) Digitale Wertrechte

Die DLT bietet weiter die Gelegenheit, den klassischen Vermögenswerten eine digitale Repräsentation zuzuordnen.[82] Dadurch können die Teilnehmenden Eigentumsrechte an physischen Gegenständen bzw. Gütern (z.B. Immobilien) digital auf den Distributed Ledgers hinterlegen. Nachdem ein Vermögenswert digitalisiert ist, stehen verschiedenste Optionen offen; ein interessanter Ansatz ist die Möglichkeit, den Vermögenswert in viele kleine Anteile zu unterteilen und diese an verschiedene Eigentümer zu verkaufen; dadurch wird die Implementierung neuer Arten der Finanzierung und der Vermögensverwaltung ermöglicht.[83]

e) Kapitalbeschaffung

Die Krypto-Assets können auch als alternative Methode der Kapitalbeschaffung dienen, die für die Gründung, Weiterentwicklung und/oder Expansion eines Unternehmens Verwendung zu finden vermag. Die Unternehmen haben

79 *Diehl*, 2021, Rz. 24.

80 *Diehl*, 2021, Rz. 25.

81 Vgl. hierfür Kap. II.C.4.

82 Vgl. Kap. II.B.7.

83 *Rutishauser/Kubli/Weber*, 2021, Rz. 48.

die Möglichkeit, mittels Token Generating Events (TGEs) neue Token zu schaffen (z.B. mit den Initial Coin Offerings [ICOs]) und so das Unternehmen zu finanzieren; sie bieten der Öffentlichkeit eine vordefinierte Anzahl digitaler Token (Coins) an und erhalten im Gegenzug entweder Kryptowährungen oder Fiatwährungen. Neben den ICOs hat sich auch der Begriff der Securities Token Offerings (STOs) etabliert; dabei handelt es sich um die Ausgabe von Wertpapieren. In Zahlen ausgedrückt erreichten die ICOs und STOs zusammen ein globales Volumen von USD 31.1 Mia.; den Höhepunkt hatten die ICOs und STOs im Jahre 2018 mit USD 19.7 Mia., doch sank ihr Volumen im Jahre 2019 auf USD 4.1 Mia.[84] Im Jahre 2020 erreichten die STOs ein Volumen von USD 4.8 Mia.[85]

Die FINMA hat bereits früh eine Aufsichtsmitteilung sowie eine Wegleitung für die ICOs publiziert.[86] Obwohl internationale oder schweizerische Vorschriften unmittelbar zu den ICOs fehlen, kann die FINMA aufgrund verschiedener Anknüpfungspunkte die ICOs aufsichtsrechtlich beurteilen. Angesichts der vielfältigen Ausgestaltung der ICOs ist nicht in jedem Fall eine Unterstellungspflicht gegeben, sondern eine Einzelfallbetrachtung erweist sich als erforderlich.[87] Bereits in der Aufsichtsmitteilung 04/2017 hat die FINMA potenzielle Anknüpfungspunkte zum geltenden Aufsichtsrecht herausgearbeitet:[88]

- Falls die Schaffung eines Token im Rahmen des ICO eine Ausgabe eines Zahlungsmittels darstellt, ist grundsätzlich das Geldwäschereigesetz (GwG) anwendbar. In diesen Fällen können potenziell auch weitere Unterstellungstatbestände im Rahmen des Sekundärhandels mit Tokens greifen.
- Mit dem ICO könnte auch die Entgegennahme von Publikumseinlagen und somit die Pflicht zur Bankenbewilligung einhergehen, wenn gestützt auf das ICO eine Verbindlichkeit der Betreibenden des ICO gegenüber seinen Teilnehmenden entsteht, was in der Praxis in der Regel aber nicht der Fall ist.

84 SCA, 2021, 13; *Rutishauser/Kubli/Weber*, 2021, Rz. 49 f.; für die Zahlen, vgl. *PwC/CVA*, 2020, 2 ff.

85 *Hays et al.*, 2021, 27.

86 FINMA, 2018a; FINMA, 2017a.

87 FINMA, 2018a, 2; FINMA, 2017a, 2; vgl. ferner FINMA, FINMA publiziert Wegleitung zu ICOs vom 16. Februar 2018, aufrufbar unter <https://www.finma.ch/de/news/2018/02/20180216-mm-ico-wegleitung/>.

88 FINMA, 2017a, 2 f.

- Falls die beim ICO ausgegebenen Token als Effekten zu qualifizieren sind, dürfte eine Bewilligungspflicht als Wertpapierhaus zur Anwendung kommen.
- Potenzielle Berührungspunkte zum Kollektivanlagegesetz (KAG) sind vorhanden, wenn das beim ICO gesammelte Vermögen fremdverwaltet wird.

f) Kryptoanlagen

Da sich verschiedenste Vermögensgegenstände in unterschiedlichen Kategorien tokenisieren lassen und sie auf der Blockchain handelbar sind, dürften die Investitionen in die Kryptowelt künftig Zuwachs finden.

Einerseits ist es denkbar, in verschiedenste Krypto-Anlagaprodukte (z.B. Krypto-ETFs, Krypto-ETPs, Krypto-Derivate) zu investieren, andererseits bildet sich auf der Blockchain auch ein Markt für beispielweise Kunstwerke in Form von Non-Fungible Tokens (NFTs) heraus. NFTs sind nicht vertretbare Token, die nicht teilbar und deshalb nur in der ursprünglichen Gestalt übertragbar sind; diese Eigenschaften sind für die digitale Kunst entscheidend.[89]

Die Bedeutung der NFTs wird bei Betrachtung des Handelsvolumens ersichtlich; im Jahre 2021 fanden NFT-Verkäufe von über USD 25 Mrd. statt. Einen wichtigen Teil dieser Käufe bzw. Verkäufe macht der Handel auf der Plattform OpenSea aus, die für Sammelobjekte am beliebtesten zu sein scheint.[90]

g) Verwahrung

Da bei den DLT-Systemen keine Banken oder Verwahrstellen als Intermediäre agieren bzw. existieren, haben die Teilnehmenden ihre eigenen Wallets zur Aufbewahrung ihrer digitalen Werte. Trotzdem kann es bei grösserem Vermögen aus Gründen der Sicherheit sinnvoll sein, die Vermögenswerte bei einem Custody-Provider zu hinterlegen. Denkbar ist, dass die Custody-Provider Hard Wallets, wie z.B. Festplatten, in einem Bunker in den Bergen vor Diebstahl, Schädigung durch Strahlung, Erdbeben oder anderen Einflüssen sichern. Nachteil dieser Sicherung ist der erschwerte Zugriff auf die eigene Wallet; aus

---

89 *Chohan*, 2021, 1 ff.; *Kaulartz/Schmid*, 2021, 298 ff.; *Hoeren/Prinz*, 2021, 565 ff.

90 *Elizabeth Howcroft*, NFT sales hit billion in 2021, but growth shows signs of slowing, Reuters, January 11, 2022, aufrufbar unter <https://www.reuters.com/markets/europe/nft-sales-hit-25-billion-2021-growth-shows-signs-slowing-2022-01-10/>.

diesem Grund lassen sich Hard Wallets auch bei einer Bank hinterlegen und so die Ausführung von Transaktionen erleichtern, während weiterhin eine gewisse Sicherheit gewährleistet ist. Zudem ist es bei hohem Vermögen potenziell auch sinnvoll, trotz zusätzlicher Gefahrenquellen sichere Backups der Zugangsschlüssel zu erstellen, da bei Verlust der Zugangsdaten der Zugriff auf die Wallet nicht mehr möglich ist.[91]

h) Weitere Bereiche

Die Blockchain bietet nicht nur im Bereich der Finanzindustrie vielversprechende Lösungen an, sondern auch im Kontext von Lieferketten (z.B. bei Lebensmitteln, Edelmetallen oder Rohstoffen). Darüber hinaus sind auch Blockchain-Lösungen im Rahmen der Musikindustrie denkbar, insbesondere in Verbindung mit den Rechten an den Titeln und der (automatisierten) Bezahlung der Künstlerinnen und Künstler. Da diese Themen jedoch ausserhalb der hier behandelten Fragen liegen, ist nicht weiter darauf einzugehen.

4. Bedeutung der DLT für Handelsplätze im Besonderen

Ein wichtiger Bestandteil jedes Finanzsystems ist ein Mechanismus zur Eigentumsübertragung von Vermögensgegenständen; solche Transaktionen finden auf sogenannten Handelsplätzen statt. Ein Handelsplatz erfüllt grundsätzlich folgende vier Funktionen: (i) Kapitaleinzahlung, (ii) Verwaltung des Orderbuchs, (iii) Abgleich der ausgeführten Orders und (iv) Eigentumsüberwachung der Vermögenswerte.[92]

In der «traditionellen» Finanzwelt existieren ausschliesslich zentralisierte Handelsplätze; diese sind auch in der Krypto-Welt anzutreffen. Der Vorteil zentralisierter Handelsplätze ist, dass sie die Kontrolle über das User Interface haben und dadurch Laien ohne Komplikationen Transaktionen tätigen können; sie sind also nutzerorientiert, leicht zu bedienen und bieten eine gute Liquidität für die gängigsten Kryptowährungen. Oft sind diese Handelsplätze auch offen, den Wünschen der Nutzerinnen und Nutzer nachzukommen und Funktionen einzubauen; im Gegenzug sind die Nutzerinnen und Nutzer dazu verpflichtet, Gebühren zu zahlen, damit die Betreibenden das System am Laufen halten können.[93]

---

91 *Rutishauser/Kubli/Weber*, 2021, Rz. 59.

92 *Rutishauser/Kubli/Weber*, 2021, Rz. 52.

93 *Rutishauser/Kubli/Weber*, 2021, Rz. 53.

Einige Handelsplätze bieten gelichzeitig eine Verwahrung der digitalen Werte an, sodass die Nutzenden von der Aufgabe entlastet sind, selbst für die Verwahrung sorgen zu müssen. Diese Dienstleistung erhöht die Nutzerfreundlichkeit der Handelsplätze, da die Nutzenden keinen separaten Private Key benötigen, sondern mit Benutzername und Passwort bereits auf ihr Vermögen zugreifen können.[94]

Im Gegensatz zu den zentralisierten Handelsplätzen werden bei dezentralen Handelsplätzen die zuvor erwähnten vier Grundfunktionen eines Handelsplatzes dezentral ausgeführt. Der (wohl) bekannteste dezentrale Handelsplatz ist Uniswap; er hat fast alle wirtschaftlich bedeutenden ERC-20 Token gelistet. Uniswap ermöglicht unter anderem den direkten Handel zwischen ERC-20/ERC-20-Paaren und erlaubt mit dem Governance-Token auch eine dezentralisierte Konsensbildung.[95]

[94] Zur Unterscheidung zwischen Hot Wallets und Cold Wallets sowie zu den Sicherungsmöglichkeiten vgl. Kap. II.B.4; *Rutishauser/Kubli/Weber*, 2021, Rz. 54.

[95] *Rutishauser/Kubli/Weber*, 2021, Rz. 58.

III. Regulatorische Rahmenordnung für DLT-Handelsplattformen

A. Einleitung

Wie dargelegt, ist es durch die DLT möglich, digitalen Aktiven (bzw. das digitale Vermögen) ohne Intermediäre zu besitzen und zu transferieren; zudem erlaubt die DLT die Tokenisierung solcher Vermögen. Der Token gilt im Rahmen der Distributed Ledgers als digitale Repräsentation eines Gutes und kann wie Assets, die Teil des zugrundeliegenden Protokolls sind, gehandelt werden.[96] Ein wichtiges Beispiel der Tokenisierung ist die Schaffung digitaler Aktiven; sie ist nur der erste Schritt mit Blick auf die Realisierung neuer DLT-basierter Geschäftsmodelle. Die geschaffenen digitalen Aktiven müssen weiter auch verkehrsfähig sein, d.h. gehandelt werden können. Der Gesetzgeber hat deshalb einen zentralen Bereich des DLT-Gesetzes den neuen Rahmenbedingungen für den (Sekundär-)Handel mit digitalen Aktiven und folglich auch der Schaffung von Handelsplattformen gewidmet.[97]

1. Begriffe

Die neuen Bestimmungen zum Handel mit digitalen Aktiven erfordern begriffliche Klarstellungen, insbesondere mit Bezug auf die DLT-Effekten und die DLT-Handelssysteme.

a) DLT-Effekten

Die zivilrechtlich neu geschaffenen Registerwertrechte (Art. 973d OR) haben zu einer Ergänzung des Begriffs der Effekten geführt; unter den Begriff der Effekten fallen gemäss Art. 2 lit. b FinfraG nun auch die Registerwertrechte.

---

96 Vgl. weiterführend zur Tokenisierung Kap. II.B.7.

97 Der nachfolgende Text basiert auf *Rolf H. Weber*, Handel mit digitalen Aktiven. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 165–197 (*Weber*, 2021a), enthält aber Aktualisierungen auf den neuesten Stand der Regelungen; dieser Beitrag wird nachfolgend nicht weiter referenziert. Für einen Überblick zum neuen DLT-Gesetz vgl. den Sammelband von *Rolf H. Weber/Hans Kuhn* (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021.

Die DLT-Effekten sind in Art. 2 lit. b^{bis} FinfraG definiert: Einerseits gelten Effekten in der Form von Registerwertrechten als DLT-Effekten (Ziff. 1). Andererseits sind auch Effekten von anderen in verteilten elektronischen Registern gehaltenen Wertrechten, die den Gläubigerinnen und Gläubigern, nicht aber den Schuldnerinnen und Schuldnern, mittels technischer Verfahren die Verfügungsmacht über die Wertrechte vermitteln, als DLT-Effekten definiert (Ziff. 2). Die zweite Alternative soll im Sinne der Technologieneutralität[98] die Schaffung bisher noch nicht bekannter DLT-Effekten ermöglichen.[99] Der Gesetzgeber beabsichtigt mit der Aufnahme des Zusatzes «andere Wertrechte» z.B. auch nach ausländischem Recht geschaffene Wertrechte als DLT-Effekten abzudecken; eine Sonderregelung hierfür wäre aber nicht erforderlich, da die ausländischen Instrumente nach kollisionsrechtlicher Praxis ohnehin erfasst wären.

Gemäss der Legaldefinition in Art. 2 lit. b^{bis} FinfraG sind DLT-Effekten immer auch Effekten und somit Finanzinstrumente im Sinne des FIDLEG (Art. 3 lit. b FIDLEG). Im Gegensatz zu traditionellen Effekten und Bucheffekten, die sich nur unter Mitwirkung eines Intermediärs übertragen lassen, können DLT-Effekten auch von Inhaberinnen und Inhabern direkt auf Dritte übertragen werden.[100]

DLT-Effekten vermitteln auf der Basis technischer Verfahren die rechtliche Verfügungsmacht. Für die Erfüllung des Begriffs der DLT-Effekten ist entscheidend, dass die auf der Grundlage von anderen Wertrechten geschaffenen DLT-Effekten in verteilten elektronischen Registern gehalten werden und die Gläubigerinnen und Gläubiger durch technische Verfahren die Verfügungsmacht über das Wertrecht erhalten. Die Wertrechte bzw. DLT-Effekten lassen sich somit auch nach ausländischem Recht begründen.[101]

Der Begriff der DLT-Effekten umfasst nicht die sog. Zahlungs-Token und Nutzungs-Token.[102] Diese Beurteilung ist bei Zahlungs-Token, welche Kryptowährungen repräsentieren, offensichtlich. Nutzungs-Token hingegen können zwar in der Form von Wertrechten bzw. den neuen Registerwertrechten ausgegeben werden; vermitteln die Nutzungs-Token jedoch ausschliesslich Anspruch auf Zugang zu einer digitalen Dienstleistung oder Nutzung, qualifizieren sie

98 *Kuhn/Weber*, 2021, Rz. 20 ff.

99 Botschaft DLT-Gesetz, BBl 2020, 309.

100 *Eggen/Sillaber*, 2020, Rz. 5.

101 Botschaft DLT-Gesetz, BBl 2020, 309.

102 Für weitere Ausführungen zur Kategorisierung von Token, vgl. Kap. II.B.7.

nicht als Effekten. In der Praxis stellt sich indessen das Problem, dass oft «hybride Token» anzutreffen sind, die mehrere Funktionalitäten aufweisen; die von der FINMA vorgenommene aufsichtsrechtliche Kategorisierung ist deshalb materiell zum Teil nicht weiterführend.[103] Obwohl der Ausschluss der Zahlungs- und Nutzungs-Token aus der Legaldefinition in Art. 2 lit. b^{bis} FinfraG der Praxis der FINMA entspricht, hat diese Ausklammerung somit nur einen beschränkten Nutzen, da die effektive Unterscheidung zwischen den Token-Kategorien sehr unscharf verläuft. Anzumerken gilt immerhin, dass DLT-Handelssysteme neben DLT-Effekten ebenso andere Vermögenswerte (z.B. Nutzungs- oder Zahlungs-Token) zum Handel anbieten können.[104]

Der Begriff der DLT-Effekten erfasst auch nicht die «klassischen» Effekten, die sich auf einen DLT-basierten Vermögenswert beziehen, etwa ein traditionelles Derivat mit einer Kryptowährung als Basiswert oder ein Exchange Traded Product mit kryptobasierten Vermögenswerten als Basiswerten.[105]

b) Wertrechteregister

aa) Eigenschaften

Als Registerwertrecht lässt sich jedes Recht ausgestalten, das auch als Wertpapier ausgestaltbar ist, also obligatorische Rechte, Mitgliedschaftsrechte (soweit vom Gesetz erlaubt) und einzelne Sachenrechte; nicht vorausgesetzt ist die Vertretbarkeit des abgebildeten Rechts.[106] Diejenigen Funktionen, die traditionell von Wertpapieren und Bucheffekten erfüllt werden, sind auch den Registerwertrechten inhärent, nämlich die Transport-, Legitimations- und Verkehrsschutzfunktion.[107]

Registerwertrechte bedürfen der Eintragung im Wertrechteregister. Gemäss Art. 973d OR muss ein Wertrechteregister vier zentrale Anforderungen erfüllen:[108]

---

103 Vgl. hierzu Kap. II.B.7; für eine Auseinandersetzung mit den verschiedenen Tokenarten *Weber/Baisch*, 2021, 684 f.; *Weber/Baisch*, 2019a, 141 f.

104 Botschaft DLT-Gesetz, BBl 2020, 309 f.

105 Botschaft DLT-Gesetz, BBl 2020, 310.

106 *Weber*, 2021e, Rz. 10.

107 Botschaft DLT-Gesetz, BBl 2020, 259; *Kuhn*, 2021a, Rz. 24 ff.; *Weber*, 2021e, Rz. 11; *Kramer/Meier*, 2020, 62; *von der Crone/Derungs*, 2019, 492.

108 *Kuhn*, 2021a, Rz. 54 ff.; *Weber*, 2021e, Rz. 14-16.

- Einräumung der faktischen Möglichkeit an die Gläubiger, nicht aber an den Schuldner, mittels technischer Verfahren über die Rechte zu verfügen (sog. Verfügungsmacht);
- Schutz der Integrität des Wertrechteregisters durch angemessene technische und organisatorische Massnahmen;
- Schaffung von Transparenz hinsichtlich des Inhalts der Rechte, der Funktionsweise des Registers und der Registrierungsvereinbarung;
- Einräumung von Einsichts- und Verifikationsrechten an die Gläubiger.

Erfüllt ein «Register» diese Anforderungen nicht, fehlt dem eingetragenen Recht die Qualität des Registerwertrechts und es kann insbesondere nicht nach den Regeln von Art. 973f OR rechtsgültig übertragen werden, d.h. der Käufer erwirbt kein Eigentum. Die Einhaltung der technischen und organisatorischen Massnahmen durch den Anbieter des Wertrechteregisters ist deshalb von entscheidender Bedeutung.[109]

bb) Wirkungen

Das Wertrechteregister muss den Gläubigern, nicht aber dem Schuldner, die Verfügungsmacht über seine Rechte mittels technischer Verfahren vermitteln. Aus der Botschaft geht hervor, dass Wertrechteregister die Verfügungsmacht nur *im Grundsatz* mittels technischer Verfahren zu ermöglichen haben; sie sind insbesondere nicht gehalten, den Gläubigern *jederzeit* die Verfügung über die Registerwertrechte sicherzustellen.[110] Das vorübergehende Ausfallen des Wertrechteregisters (z.B. aufgrund von Wartungsarbeiten, Netzwerkstörungen oder Hackerangriffen) berührt die Wertpapierwirkung der Registerwertrechte nicht.[111]

c) DLT-Handelssysteme

Ein DLT-Handelssystem ist «eine gewerbsmässig betriebene Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie den Vertragsabschluss nach nicht-diskretionären Regeln bezweckt» (Art. 73a Abs. 1 FinfraG). Zwar ist die gesetzliche Umschreibung des DLT-Handelssystems ähnlich wie die Begriffs-

109 Im Einzelnen dazu *Kuhn*, 2021a, Rz. 72 ff.

110 Botschaft DLT-Gesetz, BBl 2020, 279.

111 Vgl. auch *Kuhn*, 2021a, Rz. 58; *Kramer/Meier*, 2020, 63.

bestimmung der Börse (Art. 26 lit. a FinfraG); im Gegensatz zu traditionellen Börsen und multilateralen Handelssystemen ermöglicht ein DLT-Handelssystem bei Erfüllung bestimmter Voraussetzungen den Handel mit DLT-Effekten, schliesst gleichzeitig aber die Erbringung weiterer Dienstleistungen nicht grundsätzlich aus.[112]

DLT-Handelssysteme sind somit eigenständig organisierte Handelsplätze für DLT-Effekten und weitere digitalen Aktiven. Abgrenzungsprobleme zu konventionellen Handelsplätzen sind aber nicht vollständig ausser Acht zu lassen, weil die Abwicklung auf DLT-Handelssystemen sich auch zentral organisieren lässt.

Die konkreten Anforderungen an ein DLT-Handelssystem ergeben sich aus Art. 73a FinfraG und Art. 12 Abs. 2 FinfraV.

2. Bedeutung der neuen Regulierungen

Die neuen Bestimmungen zum Handel mit digitalen Aktiven haben eine grosse rechtliche und wirtschaftliche Bedeutung. Damit sich die neuen DLT-Geschäftsmodelle erfolgreich entwickeln und ausbreiten können, müssen die digitalen Aktiven individuell und gewerbsmässig von einer Person auf eine andere Person übertragbar sein. Nach der Schaffung von digitalen Aktiven und deren Zuordnung zu einzelnen Inhaberinnen und Inhabern setzen wirtschaftlich erfolgreiche Geschäftsmodelle auch voraus, dass ein Wechsel der Inhaberschaft durch einen transaktionalen Vorgang möglich ist.

Die Schweiz gehört weltweit zu den ersten Ländern, die angemessene Rahmenbedingungen für den Handel mit digitalen Aktiven geschaffen hat. Die damit bewirkte Rechtssicherheit ist ein Standortvorteil, dessen Bedeutung nicht zu unterschätzen ist.

[112] Botschaft DLT-Gesetz, BBl 2020, 311. Die FINMA hat die SIX Digital Exchange (SDX), die mit einer vollständig regulierten, integrierten Handels-, Abwicklungs- und Verwahrungsinfrastruktur basierend auf der DLT in Betrieb geht, als Börse und Zentralverwahrer bewilligt (FINMA, Medienmitteilung – FINMA bewilligt erstmals Börse und Zentralverwahrer für Handel mit Token vom 10. September 2021).

B. Notwendige Neukonzeption des Handels mit digitalen Aktiven

1. Ungenügen des geltenden Rechtsrahmens

Das FinfraG, in Kraft seit anfangs 2016, kennt grundsätzlich drei Formen von Handelssystemen, nämlich die traditionellen Börsen (Art. 26 lit. b FinfraG), die multilateralen Handelssysteme (Art. 26 lit. c FinfraG) und die organisierten Handelssysteme (Art. 42 FinfraG). Der Handel von digitalen Aktiven auf der Basis der DLT ist auf diesen Plattformen bisher nicht zugelassen worden. Die Praxis hat auch gezeigt, dass ungeachtet vielfältig geschaffener digitaler Aktiven in den letzten Jahren ein eigentlicher Handel mit diesen Werten noch kaum zustande gekommen ist.

Das FinfraG geht traditionell von einem «klassischen» Bild zentral organisierter Finanzmarktinfrastrukturen aus, was dazu führt, dass sich für den dezentralen Handel ein Anpassungsbedarf ergibt.[113] Das heutige Recht erlaubt beispielsweise (abgesehen von beschränkten Ausnahmen) einem Finanzintermediär lediglich den Betrieb eines einzigen multilateralen Handelssystems (Art. 10 FinfraG). Die Geschäftsmodelle im Bereich DLT und Blockchain sind nicht ohne Weiteres in dieses Regulierungsregime einzuordnen. Um eine grössere Rechtssicherheit herbeizuführen, hat sich der Gesetzgeber zutreffend entschieden, die neue Rechtsform der DLT-Handelsplattformen zu schaffen.

Immerhin ist nicht zu übersehen, dass die Abwicklungstätigkeiten im Kontext von DLT-Handelsplattformen mit den bisher geltenden Bestimmungen des FinfraG zum Nachhandel wohl vereinbar gewesen wären. Aufgrund der breiten Legaldefinition lässt sich nämlich die Abwicklung und Verwahrung von DLT-Effekten mittels Smart Contract[114] als auf «einheitlichen Regeln und Verfahren» (Art. 48 FinfraG) beruhend qualifizieren.

Die Erarbeitung und Inkraftsetzung spezifischer Bestimmungen für DLT-Handelssysteme erweist sich dennoch als sachgerecht und angezeigt.

---

113 Börsen und andere Handelssysteme dienen der Konzentration von Kaufs- und Verkaufsangeboten an einer *zentralen Stelle* (vgl. Botschaft FinfraG, BBl 2014, 7489); zudem regelt das FinfraG zentrale Gegenparteien (Art. 48 ff. FinfraG) und Zentralverwahrer (Art. 61 ff. FinfraG).

114 Für Details zu den Smart Contracts, vgl. Kap. II.B.5.

2. Überblick über die neuen Bestimmungen

Abgesehen von der bereits erwähnten Anpassung der Definitionen (DLT-Effekten, DLT-Handelssysteme) hat das DLT-Gesetz vor allem ein neues Kapitel 4a in das FinfraG aufgenommen (umfassend die Art. 73a–73f FinfraG). Der Inhalt dieser neuen Bestimmungen umfasst insbesondere folgende Aspekte:

- Umschreibung und Konkretisierung des Begriffs des DLT-Handelssystems und der Gewerbsmässigkeit (Art. 73a FinfraG);
- Geltung bestimmter für Handelsplätze aufgestellter Anforderungen auch für DLT-Handelssysteme (Art. 73b FinfraG);
- Zulassung von Teilnehmerinnen und Teilnehmern sowie deren Pflichten (Art. 73c FinfraG);
- Zulassung von DLT-Effekten und weiteren Vermögenswerten (Art. 73d FinfraG);
- Weitere Anforderungen, denen die DLT-Handelssysteme zu genügen haben, insbesondere mit Blick auf die finanzielle Ausstattung und die Ausübung der Tätigkeiten (Art 73e FinfraG);
- Erleichterungen für kleine DLT-Handelssysteme (Art. 73f FinfraG).

Die gesetzlichen Bestimmungen werden durch eine grössere Zahl von Verordnungsbestimmungen ergänzt, insbesondere Art. 58a–58o FinfraV (ebenfalls neues Kapitel 4a der FinfraV).[115] Ausserdem hat die FINMA eine umfangreiche Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem nach Art. 73a ff. FinfraG erlassen.[116]

3. Vergleich mit ausländischen Rechtsentwicklungen

Die Schweiz ist mit den Bestimmungen zu den DLT-Handelssystemen einen grossen Schritt vorangegangen, der im Ausland noch nicht in dieser Weise erfolgt ist.

---

115 Im BIS Working Paper No. 1015 unterscheiden die Autorinnen und Autoren im Kontext der Regulierungsansätze zwischen der «Ledger Perspective» (Anpassung des Rechts an die DLT) und der «Node Perspective» (Einhaltung des geltenden Gesetzes durch die Nodes). Selbstverständlich müssen die Nodes immer die geltenden Gesetze einhalten, jedoch bezieht sich diese Unterscheidung auf den Regulierungsansatz im Allgemeinen (*Zetzsche/Anker-Sørensen/Passador/Wehrli*, 2022, 25 ff.). Die Schweiz scheint die «Ledger Perspective» beim DLT-Gesetz gewählt zu haben.

116 FINMA, 2021b.

Liechtenstein hat ein eigenes Gesetz erlassen, das auf vertrauenswürdigen Technologien (VT) basierende Transaktionssysteme regelt;[117] das Gesetz über Token und VT-Dienstleister (TVTG) ist am 1. Januar 2020[118] in Kraft getreten. Das TVTG enthält eine Legaldefinition für DLT-Handelssysteme («VT-Systeme») in Art. 2 Abs. 1 lit. b TVTG; es regelt hauptsächlich die Beaufsichtigung von «VT-Dienstleistern»[119] (Art. 11–49 TVTG), nicht jedoch die VT-Systeme selbst. Als EWR-Mitglied ist Liechtenstein verpflichtet, den Finanzmarkt-Acquis zu übernehmen und kann nicht in diesen eingreifen; das TVTG enthält deshalb einen entsprechenden Vorbehalt. Anders als die Schweiz hat der Liechtensteiner Gesetzgeber ein gänzlich neues Gesetz geschaffen. Über die Auswirkungen dieses Gesetzes in der Praxis lassen sich gegenwärtig noch keine abschliessenden Aussagen machen.

Die Europäische Union beabsichtigt mit der MiCA-Verordnung eine vollständige Harmonisierung der DLT-Entwicklungen.[120] In Anlehnung an die neue Schweizer Gesetzgebung sollen auch in der Europäischen Union die DLT-Handelssysteme grundsätzlich geregelt sein.[121] Die voraussichtlich im Jahre 2023 in Kraft tretende europäische Verordnung zu den Kryptowerten (MiCA-Verordnung) sieht in Art. 68[122] einzelne Anforderungen zum Betrieb der Handelsplattformen vor. Abgesehen davon liegt der Fokus der MiCA-Verordnung aber auf der Regulierung des Primärmarktes; zudem fehlt beispielsweise eine korre-

117 Vgl. weiterführend zum Gesetz in Liechtenstein *Kuhn*, 2021b, Rz. 43 ff.

118 Gesetz über Token und VT-Dienstleister vom 3. Oktober 2019 (LR-Nr. 950.6; Stand am 1. April 2021).

119 Vgl. Legaldefinition der «VT-Dienstleister» in Art. 2 Abs. 1 lit. i TVTG.

120 Vgl. weiterführend zur aufsichtsrechtlichen Entwicklung in der Europäischen Union *Kuhn*, 2021b, Rz. 6 ff.

121 Vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM/2020/593 final, 7; Europäische Kommission, Commission staff working document, impact assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, SWD(2020) 380, 34.

122 Vgl. auch Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM/2020/593 final, 15. Der Trilog zwischen den gesetzgebenden Organen ist bereits abgeschlossen; der Europäische Rat und das Europäische Parlament müssen die MiCA nur noch formal annehmen (vgl. Rat der EU, Digitalisierung des Finanzwesens: Einigung über die europäische Verordnung über Kryptowerte (MiCA) – Pressemitteilung vom 30.06.2022, aufrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.

spondierende Norm zu Art. 73f FinfraG über kleine DLT-Handelssysteme. Die Vorreiterrolle und die Bedeutung des Standorts der Schweiz zeigt sich darin, dass die Europäische Kommission an verschiedenen Orten direkt auf die schweizerische Regelung hinweist.[123]

In der Europäischen Union ist zudem die EU-DLT-Pilotregelung zu beachten, die im Sommer 2022 in Kraft getreten ist.[124] Sie schafft eine kontrollierte Umgebung für Experimente, die gewisse Ausnahmen von der Einhaltung bestimmter Vorschriften im Kontext des Finanzmarktes geniesst. Gemäss Art. 4 EU-DLT-Pilotregelung unterliegen DLT-Marktinfrastrukturen der Europäischen Finanzmarktverordnung[125] und der Richtlinie 2014/65/EU[126] für ein multilaterales Handelssystem. Die Pilotregelung sieht vor (ähnlich wie die Schweiz[127]), natürliche und juristische Personen zum Handel für eigene Rechnung als Mitglieder oder Teilnehmer zuzulassen, sofern diese Personen bestimmte Anforderungen erfüllen (Art. 4 Abs. 2 EU-DLT-Pilotregelung). Ferner legt die EU-DLT-Pilotregelung zusätzliche Anforderungen fest, die für DLT-Marktinfrastrukturen gelten, um so den Risiken im Rahmen der DLT zu begegnen (Art. 6 EU-DLT-Pilotregelung); diese Regelung hat den Fokus insbesondere auf der Bereitstellung von Informationen.[128]

Ebenso hat die International Organization of Securities Commissions (IOSCO) Grundsätze aufgestellt, die in die jeweiligen Gesetzgebungen einfliessen sollten.[129] Im Bericht zu den Regelungsaspekten bei Kryptowerten vom Februar 2020 erwähnt die IOSCO als relevante Grundsätze z.B. die Zusammenarbeit der Staaten untereinander (IOSCO Grundsätze 13-15), Prinzipien für den Sekundärmarkt und andere Märkte, wie z.B. Bewilligungspflichten und Transpa-

123 *Europäische Kommission*, Impact Assessment, 2020, 29, 48 und 60.

124 Verordnung (EU) 2022/858 des Europäischen Parlaments und des Rates über eine Pilotregelung für auf Distributed-Ledger-Technologie basierende Marktinfrastrukturen und zur Änderung der Verordnungen (EU) Nr. 600/2014 und (EU) Nr. 909/2014 sowie der Richtlinie 2014/65/EU vom 30. Mai 2022, ABl. L 151, 1–33.

125 Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 Text von Bedeutung für den EWR vom 15. Mai 2014, ABl. L 173, 84–148.

126 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU Text von Bedeutung für den EWR (Neufassung) vom 15. Mai 2014, ABl. L 173, 349–496.

127 Vgl. Kap. III.C.1.b) und IV.C.1.a).

128 Weiterführend zu den Risiken im Rahmen der DLT, vgl. Kap. IV.B.

129 IOSCO, Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, Final Report, Februar 2020, 2.

renz (IOSCO Grundsätze 33-37) sowie Vorgaben für Intermediäre, Abwicklungen und Abrechnungen (IOSCO Grundsätze 29-32 und 38). Auch die IOSCO sieht keine besonderen Bestimmungen oder Erleichterungen für kleine DLT-Handelssysteme vor.

C. DLT-Handelssysteme

1. Anforderungen an DLT-Handelssysteme

Ein DLT-Handelssystem zeichnet sich als Finanzmarktinfrastruktur dadurch aus, dass Handelsdienstleistungen für DLT-Effekten angeboten werden. Der Begriff ist aber nicht eng zu verstehen, das Angebot von Nachhandelsdienstleistungen ist zulässig.

a) DLT-Handelssysteme und traditionelle Handelssysteme

Ein DLT-Handelssystem weist Ähnlichkeiten zum multilateralen Handelssystem (Art. 26 FinfraG) auf; aus diesem Grunde wird es als Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmenden sowie den Vertragsabschluss nach nicht-diskretionären Regeln bezweckt, umschrieben.[130]

Die Abgrenzung der DLT-Handelssysteme zu den traditionellen Handelsplätzen erscheint zunächst einfach, weil eine Differenzierung zwischen den DLT-Effekten und den bisher schon gehandelten Effekten vorgenommen werden kann. Die Abgrenzung erfährt aber dann eine Durchbrechung, wenn der Handel mit DLT-Effekten nicht auf einem DLT-Handelssystem abläuft. Gemäss den gesetzlichen Vorgaben ist ein solcher Handel über eine gewöhnliche Börse möglich, da Art. 2 lit. b FinfraG auch Registerwertrechte nach Art. 973d OR als Effekten i.S. des FinfraG bezeichnet und Art. 73a Abs. 1 lit. b FinfraG davon ausgeht, dass DLT-Effekten zentral verwahrt werden dürfen. Dementsprechend haben börsen- und multilaterale Handelssysteme ebenfalls die Möglichkeit, ihre Plattformen für den Handel mit DLT-Effekten zu öffnen. Die neuen Bestimmungen des Kapitel 4a FinfraG erscheinen deshalb als nicht zwingend anwendbare *lex specialis* zu den Regeln für traditionelle Handelsplätze.

Für die Abgrenzung zwischen DLT-Handelssystemen und traditionellen Handelsplätzen lässt sich damit festhalten:

130 Botschaft DLT-Gesetz, BBl 2020, 311.

- Sofern keine DLT-Effekten gehandelt werden, ist eine Bewilligung als traditionelle Börse oder multilaterales Handelssystem notwendig.
- Handelsplätze, die den Handel mit DLT-Effekten ermöglichen, haben aufsichtsrechtlich die Wahl, ob sie sich als gewöhnlicher Handelsplatz oder als DLT-Handelssystem bewilligen lassen wollen; wird die Form des DLT-Handelssystems gewählt, lassen sich DLT-Effekten und Nicht-Effekten handeln, doch muss eine der drei weiteren Voraussetzungen von Art. 73a lit. a–c FinfraG erfüllt sein.
- Will sich der Inhaber von DLT-Effekten direkt am Handel beteiligen, bleibt nur die Wahl der Form des DLT-Handelssystems, weil die Betreiberin der Erleichterung von Art. 73a lit. a FinfraG bedarf.
- Ebenfalls nur die Form des DLT-Handelssystems kommt in Frage, wenn die Betreiberin nachgelagerte Aktivitäten wie die Verwahrung oder die Abwicklung von DLT-Effekten unterstützen will, weil dafür die Ausnahmenregelung von Art. 73a lit. b oder lit. c FinfraG in Anspruch genommen werden muss.

Aus den vorerwähnten Gründen eignen sich die gehandelten Finanzinstrumente nur beschränkt als Abgrenzungsmerkmal zwischen DLT-Handelssystemen und herkömmlichen Handelsplätzen. Vielmehr sind für die Abgrenzung die Voraussetzungen von Art. 73a lit. a–c FinfraG massgeblich. Ein DLT-Handelssystem hat mindestens eine der in lit. a–c genannten Eigenschaften aufzuweisen und verfügt damit zwingend über ein Merkmal, das in Bewilligungsverfahren für traditionelle Handelsplätze nicht vorhanden ist. In der Lehre wird deshalb zutreffend auf einen Zirkelschluss in der Argumentation der Botschaft hingewiesen:[131] Die regulatorischen Erleichterungen für den Einsatz der DLT-Technologie werden als Voraussetzungen formuliert, damit die entsprechende Regulierung zur Anwendung gelangt, was zur Folge hat, dass die Abgrenzung zu den traditionellen Handelsplätzen zwar möglich bleibt, aber darauf verzichtet wird, zu verlangen, dass der Handel und die Abwicklung über DLT-Handelssysteme dezentral erfolgen.

131 *Eggen/Sillaber*, 2020, Rz. 17.

b) Wesensmerkmale der DLT-Handelssysteme

Wie bereits erläutert ist das DLT-Handelssystem eine Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmenden sowie den Vertragsabschluss nach nicht-diskretionären Regeln bezweckt (Art. 73a Abs. 1 FinfraG) sowie mindestens eine von drei Voraussetzungen erfüllt, nämlich die Teilnehmerzulassung (vgl. Art. 73c Abs. 1 lit. e FinfraG), die zentrale Verwahrung von DLT-Effekten gestützt auf einheitliche Regeln und Verfahren oder die einheitliche Abrechnung und Abwicklung von Geschäften mit DLT-Effekten.

Der Bundesrat konkretisiert das DLT-Handelssystem als neue Finanzmarktinfrastruktur in den neuen Art. 12 Abs. 2 lit. f und g FinfraV. Die Bestimmungen zeigen in nicht abschliessender Weise die wesentlichen Dienstleistungen einer Finanzmarktinfrastruktur. Einerseits bezeichnet Art. 12 Abs. 2 lit. f FinfraV die wesentlichen Charakteristiken von DLT-Handelssystemen, die ausschliesslich Dienstleistungen im Handel erbringen, andererseits enthält Art. 12 Abs. 2 lit. g FinfraV zusätzliche Bestimmungen für DLT-Handelssysteme, die auch weitere Dienstleistungen im Bereich der Verwahrung, der Abrechnung oder Abwicklung erbringen.[132]

Die Dienstleistungen nach Art. 12 Abs. 2 lit. f und g FinfraV sind kumulativ wesentlich, falls ein DLT-Handelssystem sowohl Dienstleistungen im Handel mit DLT-Effekten als auch hinsichtlich deren Verwahrung, Abrechnung oder Abwicklung erbringt.[133]

Das DLT-Handelssystem kann auch einen Dritten beauftragen, selbstständig und dauernd wesentliche Funktionen der Geschäftstätigkeit einer Handelsplattform zu erfüllen. Bei einer Auslagerung ist mit einem Dienstleistungserbringer eine Vereinbarung abzuschliessen, denn nach Art. 11 FinfraG und Art. 12 FinfraV ist vorausgesetzt, dass ein identifizierbarer Dritter (ggf. auch ein Konsortium) die verteilten elektronischen Register betreibt. Falls das DLT-Handelssystem hingegen ein von ihm unabhängiges verteiltes elektronisches Register ohne identifizierbare Betreiberin (z.B. Ethereum oder Bitcoin-Blockchain) nutzt, liegt keine Auslagerung vor. Das DLT-Handelssystem muss aber in diesem Fall immerhin im Bewilligungsverfahren und der laufenden Aufsicht

132 Vgl. auch *EFD*, 2021, 25 f.

133 *Ibid.*

darstellen können, wie es die geltenden FinfraG-Anforderungen einhält. Analog gelten diese Überlegungen für Konstellationen, in denen das DLT-Handelssystem einen Smart Contract für bestimmte Dienstleistungen nutzt.[134]

Die bisherige Regulierung der Finanzmarktinfrastruktur war vollständig auf Finanzinstitute als Teilnehmer ausgerichtet und passt deshalb nicht auf DLT-Handelssysteme bzw. auf Peer-to-Peer Systeme. Im Gegensatz zu den bisherigen multilateralen Handelssystemen können DLT-Handelssysteme – wie erwähnt – auch natürliche Personen als Teilnehmende der Transaktionsabwicklungen zulassen. Die zugelassenen (natürlichen und juristischen) Personen müssen weder Wertpapierhäuser noch andere beaufsichtigte Einheiten mit vergleichbaren technischen und operativen Voraussetzungen sein. Der in der Schweiz geltende Grundsatz, dass das «Finanzmarktrecht […] in der Schweiz grundsätzlich technologieneutral und damit in der Lage [ist], mit neuen Technologien umzugehen»,[135] ist somit insoweit nicht verwirklicht gewesen, weil «nur» Finanzinstitute von den Infrastrukturen profitieren konnten. Mit den gezielten Anpassungen und der Legaldefinition der DLT-Effekten verstärkt sich – auf der Basis real existierender Bedürfnisse – der Gedanke der Technologieneutralität.[136]

Ein DLT-Handelssystem ist berechtigt, zusätzlich zu den DLT-Effekten auch Nicht-Effekten zu handeln (z.B. Zahlungs-Token wie Kryptowährungen und Nutzungs-Token).[137] Eine ausdrückliche Klarstellung dieser wichtigen Änderung durch den Gesetzgeber wäre wünschenswert gewesen.

Ein DLT-Handelssystem muss gewerbsmässig betrieben werden (Art. 73a Abs. 1 FinfraG); Gewerbsmässigkeit ist gegeben, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt (Art. 73a Abs. 2 FinfraG). Die Einschränkung der bewilligungspflichtigen Tätigkeiten auf gewerbsmässige Angebote ist in der Vernehmlassung zu Art. 73a FinfraG intensiv diskutiert worden; der Bundesrat und hernach der Gesetzgeber haben sich dafür entschieden, wie für andere Finanzmarktintermediäre auch als regulatorisches Erfordernis der Gewerbsmässigkeit vorzusehen.[138]

134 *Ibid.*

135 Botschaft DLT-Gesetz, BBl 2020, 248.

136 *Bundesrat*, 2018, 102.

137 Botschaft DLT-Gesetz, BBl 2020, 311; so auch *Kramer/Meier*, 2020, 76; Zu den verschiedenen Token-Kategorien im Detail vgl. Kap. II.B.7.

138 Botschaft DLT-Gesetz, BBl 2020, 311.

Art. 58b Abs. 1 FinfraV umschreibt die Gewerbsmässigkeit im Einzelnen. Die Verordnung stellt klar, dass ein gewerbsmässig betriebenes DLT-Handelssystem grundsätzlich den aufsichtsrechtlichen Anforderungen des Finanzmarktinfrastrukturrechts unterliegt; fehlt die Gewerbsmässigkeit, entfällt die Aufsicht, doch können andere Finanzmarktgesetze (insbesondere das GwG) zur Anwendung gelangen. Die Umschreibung der Gewerbsmässigkeit lehnt sich an Art. 19 FINIV an; sie wird anhand des Bruttoertrags, der Anzahl Vertragsparteien mit Geschäftsbeziehungen zum DLT-Handelssystem oder der Verfügungsmacht über fremde DLT-Effekten definiert. Die Begrenzung auf 20 Teilnehmende gilt nur für nicht beaufsichtigte Teilnehmende nach Art. 73c Abs. 1 lit. e FinfraG.[139]

Art. 58b Abs. 2 FinfraV regelt den Fall, dass ein nicht gewerbsmässig betriebenes DLT-Handelssystem einen Schwellenwert nach Abs. 1 überschreitet und demgemäss einer Bewilligung nach dem FinfraG bedarf. Vorgesehen ist eine Frist von 60 Tagen zur Einreichung des Bewilligungsgesuches bei der FINMA; der Betrieb lässt sich, ausser bei einer Untersagung durch die FINMA, während der Zeit der Gesuchsbearbeitung fortsetzen. Immerhin kann die FINMA, sofern es der Schutzzweck des FinfraG gebietet, der Betreiberin des DLT-Handelssystems untersagen, gewisse Tätigkeiten auszuüben (Abs. 3, ähnlich wie Art. 6 Abs. 4 BankV).[140]

c) Erbringung zusätzlicher Dienstleistungen

Wie erwähnt, darf das DLT-Handelssystem die DLT-Effekten zentral und gestützt auf einheitliche Regeln und Verfahren verwahren (Art. 73a Abs. 1 lit. b FinfraG). Einer zusätzlichen Bewilligung für die Funktion eines Zentralverwahrers bedarf der Betreiber eines DLT-Handelssystems nicht. Diese rechtliche Beurteilung begründet eine Differenz zu den klassischen Handelsplätzen; so untersagt z.B. Art. 10 FinfraG eine Kombination von Funktionen, indem angeordnet wird, dass ein Betreiber jeweils nur eine Finanzmarktinfrastruktur anbieten darf. Auch Art. 18 FinfraG will den Wettbewerb zwischen den Finanzmarktinfrastrukturen fördern.

Die Zulassung der Kombination beim DLT-Handelssystem begründet die Botschaft damit, dass dessen Betreiber auch Nachhandelsdienstleistungen anbieten können soll.[141] Diese Betrachtungsweise erscheint als sachgerecht, denn

139 *EFD*, 2021, 27.

140 *EFD*, 2021, 27 f.

141 Botschaft DLT-Gesetz, BBl 2020, 311.

eine erzwungene Trennung zwischen dem Handel und der Verwahrung bei DLT-Effekten würde für den Handel mit digitalen Aktiven eine administrative Erschwerung mit sich bringen. Hingegen ist diese Begründung weniger naheliegend für die Zulassung der zentralen Verwahrung von DLT-Effekten. Mit einer zentralen Verwahrung beim Betreiber der Handelsplattform geht nämlich das Element der Dezentralität verloren, selbst wenn nicht ausgeschlossen ist, dass die Gläubiger die Transaktionen (weiterhin) selbst auslösen können. Die Verfügungsmacht über die DLT-Effekten ist bei einer zentralen Verwahrung aber nicht zweifelsfrei gewährleistet und von der Funktionalität der DLT-Handelssysteme auch nicht gefordert; die Lehre spricht deshalb von einem legislatorischen Zugeständnis an zentral organisierte Infrastrukturträger, welche das Angebot digitaler Aktiven innerhalb ihrer bestehenden Geschäftsmodelle einsetzen wollen.[142]

d) Geltung weiterer FinfraG-Bestimmungen

Art. 73b FinfraG legt fest, dass bestimmte für Handelsplätze aufgestellte Anforderungen auch für DLT-Handelssysteme gelten. Verwiesen wird insbesondere auf bereits geregelte Anforderungen, nämlich die Selbstregulierung (Art. 27), die Organisation des Handels (Art. 28), die Vor- und Nachhandelstransparenz (Art. 29), die Sicherstellung des geordneten Handels (Art. 30), die Überwachung des Handels (Art. 31), die Zusammenarbeit zwischen Handelsüberwachungsstellen (Art. 32), die Einstellung des Handels (Art. 33 Abs. 2) und die Beschwerdeinstanz (Art. 37). Diese Liste von Art. 73b FinfraG zeigt, dass auch die (neuen) DLT-Handelssysteme einem recht engen Regulierungsregime unterstehen; kleinere Unternehmen dürften diesen Anforderungskatalog nur schwer erfüllen können. Nicht zur Anwendung kommen die Bestimmungen von Art. 34, 35 und 36 FinfraG, da für diese Regelungsbereiche spezifische Bestimmungen vorgesehen sind (Artikel 73c, 73d, 73e FinfraG).[143]

Einzelheiten werden in Art. 58c FinfraV geregelt: Art. 58c Abs. 1 FinraV erklärt Art. 24–32 und Art. 35 FinfraV als sinngemäss, also materiell unverändert, anwendbar. Vom Verweis ausgenommen sind die Bestimmungen zur Zulassung von Effekten (Art. 33 und 34 FinfraV), da die FinfraV hier spezifische Bestim-

142 *Eggen/Sillaber*, 2020, Rz. 12.

143 Botschaft DLT-Gesetz, BBl 2020, 312.

mungen für DLT-Handelssysteme und DLT-Effekten vorsieht.[144] Art. 58c Abs. 2 FinfraV führt zusätzlich noch eine besondere Regelung für die «Stornierung» von Transaktionen ein.[145]

2. Zulassungsregeln

a) Zulassung der Teilnehmerinnen und Teilnehmer

Bei der Zulassung der Teilnehmenden folgt Art. 73c Abs. 1 FinfraG den allgemeinen Vorgaben von Art. 34 Abs. 2 FinfraG. Immerhin ist als wichtiger Unterschied zu beachten, dass die DLT-Handelssysteme auch den Privatkundinnen und -kunden offenstehen (lit. e). Mit Blick auf die Bekämpfung der Risiken im Bereich der Geldwäscherei und der Terrorismusfinanzierung ist aber dieser Zugang für Privatkundinnen und -kunden davon abhängig, dass sie ausschliesslich in eigenem Namen und auf eigene Rechnung an DLT-Handelssystemen aktiv sind und keine Intermediärsfunktion wahrnehmen.[146]

Die Betreiberin eines DLT-Handelssystems ist nicht zwingend verpflichtet, einen direkten Zugang auch für nicht regulierte Teilnehmende vorzusehen, d.h. die Voraussetzung von Art. 73a Abs. 1 lit. a FinfraG muss – wie erwähnt – durch das DLT-Handelssystem jedenfalls dann nicht eingehalten werden, wenn entweder die Voraussetzung von lit. b oder von lit. c erfüllt ist. Der Gesetzgeber geht offensichtlich von der Annahme aus, dass nicht alle DLT-Effekten durch die Inhaber gehandelt werden können bzw. wollen.

Art. 73c Abs. 1 FinfraG erlaubt dem Bund, der Schweizerischen Unfallversicherungsanstalt (SUVA) und dem Ausgleichsfonds AHV/IV/EO (compenswiss) die Teilnahme an einem DLT-Handelssystem. Dieselbe Möglichkeit haben weiter nach ausländischem Recht beaufsichtigte Teilnehmerinnen und Teilnehmer (lit. b), und zwar auch für Rechnung Dritter.[147]

Ein DLT-Handelssystem ist nicht berechtigt, bei seinen über die eigene Einrichtung getätigten Geschäften mit DLT-Effekten oder anderen Vermögenswerten selbst als Gegenpartei aufzutreten. Der bilaterale Handel hat über ein organisiertes Handelssystem (OHS) zu erfolgen.[148]

---

144 Vgl. nachfolgend Kap. III.C.2.); auch EFD, 2021, 28.

145 EFD, 2021, 28.

146 Botschaft DLT-Gesetz, BBl 2020, 312.

147 *Ibid.*

148 *Ibid.*

Art. 73c Abs. 2 FinfraG hält die Auskunftspflicht der Teilnehmenden an DLT-Handelssystemen gesetzlich fest, und zwar in Anlehnung an Art. 29 FINMAG. Die Norm bezweckt, dass die sonst nicht beaufsichtigten Teilnehmenden auch erfasst sind. Die Auskunftspflicht für ausländische Teilnehmende erfolgt durch Vermittlung der Betreiberin des entsprechenden DLT-Handelssystems.[149]

Art. 73c Abs. 3 FinfraG regelt die Aufzeichnungs- und Meldepflichten; die Regelung ist notwendig, weil auch nicht beaufsichtigte Teilnehmende auf einem DLT-Handelssystem ihre digitalen Aktiven handeln können.[150]

In Art. 58d FinfraV nimmt der Bundesrat die Teilnehmenden nach Art. 73c Abs. 1 lit. e FinfraG von der Aufzeichnungs- und Meldepflicht gemäss Art. 38 und 39 FinfraG aus. Transaktionen solcher Teilnehmenden unterstehen aber weiterhin den Dokumentations- und Aufbewahrungspflichten des DLT-Handelssystems gemäss Art. 19 FinfraG. Damit das DLT-Handelssystem seinen eigenen regulatorischen Anforderungen genügen kann, wird es wohl regelmässig umfassende Auskunfts- und Dokumentationspflichten im Vertragsverhältnis zwischen DLT-Handelssystem und seinen Kunden festschreiben. Ferner ist auch die Meldepflicht nach Art. 58h Abs. 1 und 2 FinfraV zu beachten.[151]

Art. 73c Abs. 4 FinfraG überträgt die Kompetenz an den Bundesrat, die Einzelheiten über die Zulassung, die Pflichten und den Ausschluss von Teilnehmenden an DLT-Handelssystemen zu regeln. Diese Delegation soll eine rasche Anpassung der normativen Vorgaben an sich verändernde Technologien ermöglichen.[152] Gemäss Art. 73c Abs. 5 FinfraG haben die Betreiber der DLT-Handelssysteme ein Reglement zu erlassen über die Zulassung von Teilnehmenden, deren Pflichten und deren Ausschluss. Dieses Reglement unterliegt der Genehmigung durch die FINMA (Art. 73b lit. a FinfraG).

Nach Art. 58e Abs. 1 FinfraV soll das DLT-Handelssystem im Reglement nach Art. 73c Abs. 5 FinfraG bestimmen, ob und welche Teilnehmende nach Art. 73c Abs. 1 lit. e FinfraG es zulässt. Dabei präzisiert Art. 58e Abs. 2 FinfraV, dass der diskriminierungsfreie Zugang für Privatkundinnen und -kunden nicht zwingend zu gewähren ist. Das DLT-Handelssystem kann solche Teilnehmende vom Zugang ausschliessen, wenn sachliche Gründe vorliegen. Die Anforderun-

149 Botschaft DLT-Gesetz, BBl 2020, 313.

150 *Ibid.*

151 *EFD*, 2021, 28; vgl. weiterführend zur Meldepflicht Kap. III.C.2.b)aa).

152 Botschaft DLT-Gesetz, BBl 2020, 313.

gen zum diskriminierungsfreien und offenen Zugang nach Art. 18 FinfraG und Art. 17 FinfraV gelten somit nur für Teilnehmende nach Art. 73c Abs. 1 lit. a–d FinfraG.[153]

Art. 73c Abs. 6 legt fest, dass die Betreiber der DLT-Handelssysteme die Einhaltung des Reglements zu überwachen und nötigenfalls vertragliche Sanktionen vorzusehen haben. Diese Anordnung ist den Anforderungen von Art. 36 Abs. 2 FinfraG nachgebildet.

b) Zulassung von DLT-Effekten

aa) Zulassung von DLT-Effekten und weiteren Vermögenswerten

Die Zulassung von DLT-Effekten ist in Art. 73d FinfraG geregelt. Die Betreiber eines DLT-Handelssystems haben ein Reglement über die Zulassung zu erlassen, und zwar mit Blick auf den Handel als auch auf etwaige weitere Nachhandelsdienstleistungen (Abs. 1). Im Reglement festzulegen sind die Anforderungen an die DLT-Effekten und an Emittenten oder Dritte im Zusammenhang mit der Handelszulassung; von Interesse ist etwa eine durch unabhängige Dritte durchgeführte technische Prüfung der DLT-Effekten (Token-Audit) oder des zugrunde liegenden Wertrechteregisters (Art. 974d OR).[154]

Da die gleichen DLT-Effekten grundsätzlich an mehreren DLT-Handelssystemen zum Handel zugelassen sein können, muss auch die Handelsüberwachung zwischen mehreren DLT-Handelssystemen sichergestellt sein, sofern sie gleiche oder voneinander abhängige DLT-Effekten zum Handel zugelassen haben (Art. 58h Abs. 1 FinfraV). Diese Meldepflicht dient der Markttransparenz und -integrität.[155]

Mit Art. 58h Abs. 2 FinfraV soll dem Umstand Rechnung getragen werden, dass sich DLT-Effekten auch auf andere Effekten beziehen können, die auf einem Schweizer Handelsplatz zugelassen sind. So hat ein Emittent die Möglichkeit, gleichzeitig Aktien als Effekten an einer Börse traditionell zu kotieren und tokenisierte Aktien als DLT-Effekten an einem DLT-Handelssystem zuzulassen. Bei einer solchen Parallelität sind die DLT-Handelssysteme verpflichtet, sämtliche Transaktionen mit solchen DLT-Effekten dem entsprechenden Han-

153 *EFD*, 2021, 28.

154 Botschaft DLT-Gesetz, BBl 2020, 314.

155 *EFD*, 2021, 31.

delsplatz zu melden. Diese gemeldeten Daten müssen von den empfangenen Handelsplätzen in die Marktüberwachung einbezogen werden (Art. 31 Abs. 1 FinfraG).[156]

Art. 58h Abs. 3 FinfraV dient dem Datenschutz und statuiert, dass die nach Massgabe von Abs. 1 an DLT-Handelssystemen und nach Massgabe von Abs. 2 an Handelsplätzen gemeldeten Daten ausschliesslich für die Handelsüberwachung zu verwenden sind. Schliesslich delegiert Art. 58h Abs. 4 FinfraV die Regelung von Einzelheiten dieser Meldung an die FINMA.

Überdies legt Art. 73d Abs. 1 FinfraG fest, dass sich die Prospektpflicht ausschliesslich nach den Bestimmungen von Art. 55–57 FIDLEG richten. Die FINMA hat das Reglement und dessen Änderungen zu genehmigen (Art. 27 Abs. 4 FinfraG).

Lässt der Betreiber des DLT-Handelssystems auch weitere Vermögenswerte zum Handel oder zu den Nachhandelsdienstleistungen des Handelssystems zu, sind die Zulassung und die weiteren Rahmenbedingungen ebenfalls in einem Reglement festzuhalten, das von der FINMA zu genehmigen ist (Abs. 2).

Nach Art. 58f Abs. 1 FinfraV kann das DLT-Handelssystem die DLT-Effekten und die weiteren Vermögenswerte im Reglement einzeln bezeichnen oder nach ihrer Art und Funktion umschreiben.[157]

bb) Mindestanforderungen an das Register

Art. 73d Abs. 3 FinfraG enthält eine Kompetenzdelegation an den Bundesrat. Der Bundesrat ist berechtigt, Mindestanforderungen an das Register zu erlassen (lit. a), und zwar insbesondere im Interesse der Integrität und der Publizität des DLT-Handelssystems.

Die Mindestanforderungen an das Register sind in Art. 58g FinfraV konkretisiert. Gemäss Art. 58g Abs. 1 FinfraV können DLT-Effekten vom DLT-Handelssystem zugelassen werden, wenn das den DLT-Effekten zugrunde liegende verteilte elektronische Register den Mindestanforderungen von Art. 973d Abs. 2 OR entspricht. Für DLT-Effekten, die auf Registerwertrechten nach dem Obligationenrecht beruhen, ergibt sich dies aus Art. 2 lit. b^{bis} Ziff. 1 FinfraG i.V.m. Art. 973d Abs. 2 OR. DLT-Effekten können aber gemäss Art. 2 lit. b^{bis}

156 *Ibid.*

157 *EFD*, 2021, 29.

Ziff. 2 FinfraG auch auf anderer Grundlage geschaffen werden. Unterstehen diese Wertrechte ausländischem Recht, kommt Art. 973d Abs. 2 OR nicht zur Anwendung.[158]

Sollen solche DLT-Effekten an einem DLT-Handelssystem zugelassen und in den Finanzmarkt eingeführt werden, muss das Register, welche diesen Wertrechten zugrunde liegt, die Schweizer Anforderungen an die Wertrechteregister erfüllen. Dadurch wird sichergestellt, dass alle an einem DLT-Handelssystem zugelassenen DLT-Effekten vergleichbare Merkmale aufweisen, insbesondere bzgl. Integrität und Publizität des Registers. Diese Regelung dient dem Schutz der Kundinnen und Kunden.[159]

Nach Art. 58g Abs. 2 FinfraV müssen die Betreiber des DLT-Handelssystems das Register auf die Einhaltung der Anforderungen nach Art. 58h Abs. 1 FinfraV prüfen, falls das den zugelassenen DLT-Effekten zugrunde liegende Register nicht vom DLT-Handelssystem selbst betrieben wird; diese Prüfung hat vor der Zulassung zu erfolgen. Die Einhaltung der Anforderungen nach Abs. 1 ist nach der Zulassung regelmässig, mindestens einmal jährlich zu prüfen. Auch spontane, unterjährige Prüfungen lassen sich durchführen, falls besondere Vorkommnisse betreffend das Register festgestellt werden. Vorstellbare besondere Vorkommnisse sind beispielsweise Forks[160] (eine Gabelung der Kette bzw. ein neuer Strang in der Kette), Änderungen der Governance[161] oder auch Änderungen im technischen Protokoll, insbesondere betreffend den Konsensmechanismus. Kurzfristig aufkommende Vorkommnisse wie substantielle Veränderungen in der Hashrate, wenn sich diese auf das Register oder die darin abgebildeten DLT-Effekten nachteilig auswirken können, sollen ebenfalls spontane Überprüfungen ermöglichen.[162]

Inhaltlich wird sich die Prüfung mit den jeweiligen spezifischen technischen Verfahren des Registers zur Sicherstellung von Integrität und Publizität befassen müssen. Die Anforderungen der Integrität und Publizität stützen sich auf Art. 73d Abs. 3 lit. a FinfraG und Art. 973d Abs. 2 Ziff. 2–4 OR. Die Integrität umfasst auch faktische Aspekte, beispielsweise betreffend die Frage, ob die In-

158 Für die Möglichkeit zur Errichtung von DLT-Effekten nach ausländischem Recht vgl. Kap. III.A.1.a)).

159 *EFD*, 2021, 30.

160 *Bundesrat*, 2018, 22 f.; zum Begriff der Forks vgl. *Jacquemart/Meyer*, 2017, 471 ff.

161 Dabei ist insbesondere an Änderungen der Governance betreffend die Entscheidungsprozesse über Protokollanpassungen oder andere Weiterentwicklungen des Registers von grösserer Tragweite zu denken.

162 *EFD*, 2021, 30 f.

tegrität des Registers durch einzelne Gruppen (z.B. Mining Pools) negativ beeinträchtigt werden kann oder ob das Register andere Arten von erkennbaren Ausfallpunkten (Single Point of Failure)[163] oder unstatthaftem Einfluss (Single Point of Control) aufweist.[164]

Gemäss Art. 58g Abs. 2 FinfraV ist das DLT-Handelssystem für die Prüfung zuständig. Dabei kann es die Prüfung sowohl selbst durchführen als auch Dritte hierzu beiziehen. Beauftragt der Betreiber des DLT-Handelssystems einen Dritten mit der Prüfung, bleibt er verantwortlich für die sorgfältige Auswahl, Instruktion und Überwachung der beigezogenen Dritten. Somit ändert der Beizug des Dritten nichts an der aufsichtsrechtlichen Verantwortung des DLT-Handelssystems. Die aufsichtsrechtliche Prüfgesellschaft des DLT-Handelssystems (Art. 84 FinfraG; Art. 71 FinfraV; Art. 24 FINMAG) wird sich dementsprechend ein Bild über die Prüfung nach Abs. 2 machen müssen. Schliesslich informiert das DLT-Handelssystem gemäss Art. 58g Abs. 3 FinfraV seine Teilnehmerinnen und Teilnehmer über die durchgeführte Prüfung nach Abs. 2.[165]

cc) *Ausschluss bestimmter DLT-Effekten und weiterer Vermögenswerte*

Weiter ist der Bundesrat ermächtigt, festzulegen, dass bestimmte DLT-Effekten und weitere Vermögenswerte nicht zu einem DLT-Handelssystem zugelassen werden dürfen, etwa aus Gründen der Stabilität oder Integrität des Finanzsystems oder zum Schutz der Finanzmarktteilnehmerinnen und -teilnehmer (Art. 73d Abs. 3 lit. b FinfraG). Gemäss Auffassung der Botschaft will Art. 73d Abs. 3 FinfraG insbesondere als DLT-Effekten ausgestaltete Derivate vom Handel aus solchen Handelssystemen auszuschliessen, und zwar aus Gründen der Marktintegrität (oder zur Bekämpfung von Geldwäscherei- und Terrorismusfinanzierungsrisiken).[166]

Der Bundesrat konkretisiert die nicht zu DLT-Handelssystemen zugelassenen DLT-Effekten und Vermögenswerte in Art. 58f FinfraV. Gemäss Abs. 1 muss das DLT-Handelssystem im Reglement festlegen, welche DLT-Effekten und weiteren Vermögenswerte es zulässt. Falls das DLT-Handelssystem als DLT-Ef-

163 Vgl. zum eigentlichen Fehlen des Single Point of Failure aufgrund des Aufbaus der DLT-Systeme Kap. II.B.1.

164 *EFD*, 2021, 31.

165 *Ibid.*

166 Botschaft DLT-Gesetz, BBl 2020, 314.

fekten ausgestaltete Derivate zulässt, dürfen nur Produkte ohne Zeitwert- und Hebelkomponente zum Handel zugelassen werden. (Art. 58f Abs. 2 FinfraV).[167] Gestützt auf den Entwurf zur neuen FinfraV hatte das EFD angeführt, dass eine solche Zulassung die Integrität des Finanzsystems beeinträchtigen und die Umsetzung der GwG-Anforderungen erschweren könnte.[168] Zudem schreibt Art. 58f Abs. 3 FinfraV vor, dass DLT-Effekten und weitere Vermögenswerte, welche die Stabilität und die Integrität des Finanzsystems beeinträchtigen könnten, nicht zugelassen werden dürfen.

Überdies sind DLT-Effekten und Vermögenswerte, welche die Umsetzung der Anforderungen des GwG erheblich erschweren, grundsätzlich nicht zugelassen (Art. 58f Abs. 3 FinfraV). Solche Vermögenswerte sind nicht zugelassen, weil sie die Anonymität der Transaktionen erhöhen und somit die Rückverfolgung der Transaktionen erschweren oder sogar verunmöglichen.[169] Die nähere Umschreibung der DLT-Effekten und Vermögenswerte nach Art. 58f Abs. 3 FinfraV obliegt FINMA. Weiter muss die DLT-Handelsplattform im Reglement das Verfahren regeln, das einzuhalten ist, wenn die Zulassung der DLT-Effekten und weiterer Vermögenswerte entzogen wird (Abs. 4); ferner gelten die Anforderungen von Art. 34 FinfraV sinngemäss.

Art. 73d Abs. 4 legt schliesslich noch fest, dass die Betreiber der DLT-Handelssysteme die Einhaltung der Reglemente zu überwachen und bei Verstössen ggf. vertragliche Sanktionen zu ergreifen haben.

3. Zusätzliche gesetzliche Anforderungen

Gemäss Art. 73e FinfraG kann der Bundesrat für DLT-Handelssysteme weitere Anforderungen festlegen (Abs. 1). Mit konkretisierenden Vorschriften sollen insbesondere weniger erfahrene Teilnehmende einen besseren Schutz erfahren. Die Botschaft nennt als Beispiel etwa Informationspflichten zu DLT-Effekten (ähnlich den Transparenzvorgaben des FIDLEG), da private Personen

167 Im Gegensatz zum Vernehmlassungsentwurf, bei dem als DLT-Effekten ausgestaltete Derivate generell vom Handel auf einem DLT-Handelssystem ausgeschlossen waren.

168 *EFD*, 2021, 11. Diese Einschätzung lässt sich ohnehin hinterfragen, denn die Risikolage erscheint bei den DLT-Effekten nicht als wesentlich problematischer als bei traditionellen Derivaten.

169 *EFD*, 2021, 29.

nur bei den traditionellen Handelssystemen über ein Wertpapierhaus vorgehen müssen, nicht aber bei den DLT-Handelssystemen, die einen direkten Anschluss ermöglichen.[170]

Um die Wirksamkeit von Art. 73e Abs. 1 FinfraG sicherzustellen, führt der Bundesrat in Art. 58i FinfraV eine zusätzliche Informationspflicht ein. Das DLT-Handelssystem muss den zugehörigen Prospekt oder das Basisinformationsblatt zur Verfügung stellen (Abs. 1), ist aber selbst nicht verantwortlich für den Inhalt dieser Dokumente, welcher sich nach Art. 69 FIDLEG richtet. Die Pflicht beschränkt sich darauf, einen einfachen und uneingeschränkten Zugang zu diesen Dokumenten zu gewähren.[171]

Zusätzliche Informationspflichten sind in Abs. 2 festgelegt; das DLT-Handelssystem muss seine Teilnehmerinnen und Teilnehmer über seine Governance (lit. a) und die technischen Risiken, insbesondere Verlustrisiken (lit. b), informieren. An Art. 29 Abs. 2 FinfraG angelehnt, muss das DLT-Handelssystem sofort Informationen zu getätigten Abschlüssen mit weiteren Vermögenswerten veröffentlichen, um die Nachhandelstransparenz zu gewährleisten (Art. 58i Abs. 3 FinfraV).

Weiter ist in Art. 73e FinfraG eine Vielzahl von möglichen Vorgaben für die Erbringung von Dienstleistungen im Bereich der zentralen Verwahrung, Abrechnung oder Abwicklung vorgesehen (Abs. 2): Betroffen sind die zentrale Verwahrung, die Abrechnung und Abwicklung von DLT-Effekten (lit. a), Sicherheiten (lit. b), Eigenmittel (lit. c), Risikoverteilung (lit. d), Nebendienstleistungen (lit. e), Liquidität (lit. f), Verfahren bei Ausfall eines Teilnehmers (lit. g) und die Segregierung (lit. h). Alle diese Anforderungen beziehen sich auf Nebendienstleistungen (Verwahrung, Abrechnung, Abwicklung), die vom Gesetzgeber offenbar als risikobehaftet erachtet werden. Der materielle Inhalt dieser Vorgaben soll sich an den Anforderungen für die Zentralverwahrer (Art. 61–73 FinfraG) orientieren (Art. 73e Abs. 3 FinfraG).[172]

Art. 58j Abs. 1 FinfraV erklärt die Anforderungen von Art. 62–73 FinfraG und Art. 52–58 FinfraV für sinngemäss anwendbar; diese Anordnung überzeugt indessen nicht, weil sachlich betrachtet die Anwendung der verwiesenen Normen lediglich gerechtfertigt ist, wenn und soweit die DLT-Handelssysteme auch Dienstleistungen nach Art. 73a Abs. 1 lit. b oder lit. c FinfraG erbringen. Gemäss Abs. 2 ist die Segregierung nach Art. 69 FinfraG auch für DLT-Han-

170 Botschaft DLT-Gesetz, BBl 2020, 315.

171 *EFD*, 2021, 32.

172 Botschaft DLT-Gesetz, BBl 2020, 315.

delssysteme und für verteilte elektronische Register, das den DLT-Effekten zugrunde liegt, vorzunehmen, damit im Konkurs der Betreiberin des DLT-Handelssystems eine Aussonderung von Kryptowerten (entsprechend zur Anordnung von Art. 242a SchKG) ermöglicht wird. Die DLT-Handelssysteme verfügen derzeit weder über einen direkten Zugang zu einem Girokonto der SNB noch zum SIC-System. Deshalb kann das DLT-Handelssystem gemäss Art. 58j Abs. 3 FinfraV in Abweichung von Art. 65 Abs. 1 FinfraG auch ein anderes, von der FINMA beaufsichtigtes Institut für die Erfüllung einer Zahlungsverpflichtung heranziehen.[173] Die Auslegung des Begriffs der «Zentralverwahrung» hat auch Auswirkungen auf die Frage der Notwendigkeit einer Bewilligungserteilung gemäss Art. 73 FinfraG.

Gemäss Art. 58j Abs. 4 FinfraV gelten für ein DLT-Handelssystem auch kryptobasierte Vermögenswerte (z.B. Bitcoin, Ether, XCHF, tokenisiertes Zentralbankgel oder vergleichbare Vermögenswerte) als Liquidität im Sinne von Art. 67 FinfraG. Das Auseinanderfallen der Währungen der Zahlungsverpflichtung und Zahlungserfüllung ist aus Risikoerwägungen unzulässig. Deshalb kann das DLT-Handelssystem solche kryptobasierten Vermögenswerte nur einsetzen, falls die zugrundeliegende Zahlungsverpflichtung in der gleichen virtuellen Währung zu begleichen ist.[174]

Der Nutzerausschuss ist eine Anforderung des EU-Rechts (Art. 28 CSDR[175]). Er gibt den Nutzenden die Möglichkeit, «das Leitungsorgan des Zentralverwahrers in den sie betreffenden wesentlichen Belangen zu beraten» und er vertritt das Interesse der Inhaber der Wertpapiere.[176] DLT-Handelssysteme sind nicht verpflichtet, einen Nutzerausschuss einzurichten (Art. 58j Abs. 5 FinfraV), aber es steht ihnen frei, einen solchen auf freiwilliger Basis vorzusehen.

Zudem hat der Bundesrat bei der Festlegung der Anforderungen die technologiespezifischen Risiken besonders im Auge zu behalten und eine praxisnahe Ausgestaltung der Pflichten anzustreben (Art. 73e Abs. 4 FinfraG). Vorbehalten bleibt die Zuständigkeit der Schweiz. Nationalbank, die einzugreifen berechtigt ist, wenn Faktoren wie z.B. die Funktionsfähigkeit der Systeme in Frage stehen (Art. 73c Abs. 5 FinfraG).

---

173 EFD, 2021, 32 f.

174 EFD, 2021, 33.

175 Verordnung (EU) Nr. 909/2014 des Europäischen Parlamentes und des Rates zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 vom 23. Juli 2014, ABl. L 257, 1–72.

176 Einleitung zu CSDR, Rz. 37.

4. Erleichterungen für kleine DLT-Handelssysteme

Wie erläutert, enthält das Regulierungsregime für die DLT-Handelssysteme relativ weitgehende Anforderungen. Kleinere Unternehmen, die nur einen wie auch immer ausgestalteten, beschränkten Handel mit DLT-Effekten vornehmen wollen, dürften oft finanziell und administrativ nicht in der Lage sein, die strikten Vorgaben des Kapitels 4a FinfraG zu erfüllen. Aus diesem Grunde sieht Art. 73f FinfraG verschiedene Erleichterungen für kleine DLT-Handelssystem vor.

a) Kleine DLT-Handelsplattformen

Die kleinen DLT-Handelssysteme sind nicht davon befreit, eine Bewilligung bei der FINMA einzuholen. Art. 73f Abs. 1 FinfraG eröffnet aber dem Bundesrat die Möglichkeit, für kleine DLT-Handelssysteme gezielte Erleichterungen vorzusehen. Als Beispiele genannt werden die organisatorische Unabhängigkeit einer Finanzmarktinfrastruktur, die Erbringung von Nebendienstleistungen, die nach den Finanzmarktgesetzen keiner Bewilligung oder Genehmigung bedürfen, wie z.B. die Zulassung zum Handel von Zahlungs-Token oder die Unabhängigkeitsanforderungen an die Selbstregulierungsorganisation und die Beschwerdeinstanz. Zusätzlich vermag der Bundesrat für kleine DLT-Handelssysteme differenzierte Anforderungen an das Mindestkapital vorzusehen.

Art. 73f Abs. 2 FinfraG legt fest, welche DLT-Handelssysteme als klein gelten können. Die Einzelheiten der Regelungen waren in der Vernehmlassung umstritten, weshalb der heutige gesetzliche Wortlaut nach Auffassung des Bundesrats eine Kompromisslösung darstellt: Als «klein» gelten DLT-Handelssysteme, die mit Blick auf den Schutz der Finanzmarktteilnehmerinnen und -teilnehmer sowie die Funktionsfähigkeit und Stabilität des Finanzsystems geringe Risiken aufweisen. Als Anknüpfungspunkte für diese Beurteilung kommen die beschränkte Anzahl der Teilnehmenden eines DLT-Handelssystems, dessen beschränktes Handelsvolumen sowie die Elemente des beschränkten Verwahrvolumens oder beschränkten Abrechnungs- und Abwicklungsvolumens in Frage.[177]

In Art. 58k FinfraV hat der Bundesrat die Kriterien für kleine DLT-Handelssysteme festgelegt; gemäss Art. 58k Abs. 1 FinfraV gilt eine DLT-Handelsplattform als klein, wenn kumulativ:

[177] Botschaft DLT-Gesetz, BBl 2020, 316 f.

- sein Handelsvolumen mit DLT-Effekten kleiner ist als CHF 250 Mio. pro Jahr (lit. a);
- sein Verwahrungsvolumen von DLT-Effekten kleiner ist als CHF 100 Mio. (lit. b);
- sein Abwicklungsvolumen von DLT-Effekten Transaktionen im Wert von weniger als CHF 250 Mio. pro Jahr umfasst (lit. c).

Der Schwellenwert des Verwahrungsvolumen steht dabei aus der gewünschten Risikobetrachtung (Art. 73f Abs. 2 FinfraG) im Vordergrund. Die CHF 100 Mio. sind an den Schwellenwert im Bankenrecht (Art. 1b BankG) angelehnt. Da keine vergleichbaren Strukturen im In- oder Ausland bestehen, wird der Bundesrat die Entwicklungen im Auge behalten und allenfalls die Schwellenwerte anpassen müssen.[178] Ob mit der Anlehnung an das Bankenrecht angemessene Richtwerte herangezogen wurden, ist fraglich, weil die Schwellenwerte für die Praxis zu tief angesetzt sind. Auch kleinere DLT-Handelsplattformen werden z.B. das Handelsvolumen von CHF 250 Mio. pro Jahr schnell überschritten haben. Die kleineren Start-up-Unternehmen dürften deshalb von den vorgesehenen Erleichterungen nicht profitieren können und auf alternative Handelssysteme ausweichen müssen.

Sobald einer dieser Schwellenwerte überschritten wird, gilt die DLT-Handelsplattform nicht mehr als klein und muss dies gemäss Abs. 2 innerhalb von 10 Tagen der FINMA melden. Im Anschluss daran hat die DLT-Handelsplattform der FINMA innert 90 Tagen ein Bewilligungsgesuch nach den Vorschriften des FinfraG einzureichen. In jedem Fall gilt die DLT-Handelsplattform 90 Tage ab Überschreiten des Schwellenwertes nicht mehr als klein. Die Plattform kann bis zum Entscheid der FINMA die Erleichterungen nach Art. 58l Abs. 1 FinfraV weiterhin in Anspruch nehmen, aber die FINMA hat das Recht, ihr zu verbieten, während des Bewilligungsverfahrens weitere Teilnehmende aufzunehmen (Abs. 4).

Gemäss Art. 58o FinfraV[179] ist untersagt, kleinen DLT-Handelsplattformen Kredite zu gewähren. Dieser Artikel beruht auf Risikoerwägungen, da für kleine DLT-Handelsplattformen gemäss Art. 58l Abs. 2 FinfraV keine Eigenmittel- und Liquiditätsanforderungen gelten.[180] Relevanz erhält diese Vorschrift im Rah-

178 EFD, 2021, 33 f.

179 Dieser eigenständige Artikel war im Vernehmlassungsentwurf noch unter Art. 58k Abs. 4 E-FinfraV mit demselben Inhalt geregelt (vgl. auch EFD, 2020, 27).

180 Vgl. hierzu nachfolgend Kap. III.C.4.b).

men der potenziellen Kreditgewährung bei zentralwahrungsähnlichen Aktivitäten der DLT-Handelssysteme (Art. 64 FinfraG).[181] Ohne Eigenmittelanforderungen würde das Risiko erhöht, dass die kleinen DLT-Handelssysteme nicht über ausreichende Sicherheiten verfügen, um ihre laufenden Kreditrisiken vollständig zu decken (vgl. Art. 54 Abs. 1 FinfraV).

b) Erleichterungen

Art. 58n FinfraV sieht in Abweichung von Art. 13 FinfraV tiefere Schwellenwerte für kleine DLT-Handelssysteme vor. Für kleine DLT-Handelssysteme, die keine Dienstleistungen nach Art. 73a Abs. 1 lit. b oder c FinfraG erbringen, beträgt das Mindestkapital CHF 500'000 (Art. 58n lit. a FinfraV) oder alternativ 50% der Anforderungen von Art. 13 Abs. 1 lit. f FinfraV. Das Mindestkapital für kleine DLT-Handelssysteme, die Dienstleistungen nach Art. 73a Abs. 1 lit. b oder c FinfraG erbringen, beträgt 5 Prozent der verwahrten DLT-Effekten, mindestens aber CHF 500'000 (Art. 58n lit. b FinfraV). Da gemäss Art. 58k Abs. 1 lit. b FinfraV ein DLT-Handelssystem höchstens CHF 100 Mio. DLT-Effekten verwahren darf, bewegt sich das Mindestkapital somit zwischen CHF 500'000 und CHF 5 Mio.

Die konkreten Erleichterungen z.B. mit Blick auf Organisation und Mindestkapitalisierung der Handelsplattformbetreiberin sowie in der Geschäftsausübung ergeben sich aus Art. 58l und Art. 58m FinfraV. Art. 58l Abs. 1 FinfraV sieht Erleichterungen in Abweichung der FinfraG-Anforderungen vor; in lit. a und e sind z.B. Erleichterungen bzgl. des personellen Aufwands statuiert. Abs. 1 lit. b hingegen schränkt Art. 10 Abs. 3 FinfraG betreffend organisatorische Massnahmen ein; es erlaubt der FINMA zudem, falls das DLT-Handelssystem zusätzlich ein organisiertes Handelssystem betreibt, auch zusätzliche Eigenmittel als ausreichende Liquidität zu verlangen.

Die Geschäftskontinuität ist sodann laut Abs. 1 lit. c ebenso erfüllt, wenn bei Eintritt von Schadensereignissen der Betrieb des DLT-Handelssystem von einem anderen Bewilligungsträger übernommen wird (Art. 13 Abs. 1 FinfraG). Selbstredend muss der übernehmende Bewilligungsträger für die fortzuführenden Dienstleistungen aufzukommen in der Lage sein, ohne selber in Schwierigkeiten zu geraten. Zudem können die Strategie und die Geschäftsauswirkungsanalyse nach Art. 14 FinfraV vorsehen, dass der Betrieb des DLT-Handelssystems an einen Dritten übertragen wird. Ausserdem erlaubt Abs. 1 lit. d, dass die dem DLT-Handelssystem übertragenen Regulierungsaufgaben

[181] *EFD*, 2021, 35.

auch von einer nicht unabhängigen Stelle wahrgenommen werden. Von einer internen Beschwerdeinstanz kann bei kleinen DLT-Handelsplattformen ebenfalls abgesehen werden (Abs. 1 lit. e), wie auch von der internen Revision (Abs. 1 lit. f). Dabei bleibt zu beachten, dass die korrespondierenden Ausführungsbestimmungen für die kleinen DLT-Handelssystemen jeweils keine Geltung haben.[182]

Darüber hinaus gelten gemäss Abs. 2 für kleine DLT-Handelssysteme, die Dienstleistungen nach Art. 73a Abs. 1 lit. b oder c FinfraG erbringen, die Anforderungen betreffend Eigenmittel (Art. 66 FinfraG) und betreffend Liquidität (Art. 67 FinfraG) nicht.

Da kleine DLT-Handelsplattformen von diesen regulatorischen Erleichterungen in Art. 58l FinfraV profitieren, müssen sie gemäss Art. 58m FinfraV ihre Kundinnen und Kunden über die genutzten Erleichterungen orientieren. Diese Informationspflicht greift sowohl vor Aufnahme einer Geschäftsbeziehung als auch bei einer laufenden Geschäftsbeziehung, falls die beanspruchten Erleichterungen von Art. 58l FinfraV geändert werden.

5. Anhang: Weitere relevante Rechtsnormen

Abgesehen von den nachgenannten relevanten Rechtsnormen hat das DLT-Gesetz auch zu einer Änderung von Art. 154 FinfraG betr. das Ausnützen von Insiderinformationen geführt: Gemäss Abs. 1 lit. a und lit. b sowie Abs. 3 und 4 sind im Sinne einer Ergänzung und Erweiterung des Tatbestands nun auch entsprechende Handlungen mit DLT-Effekten erfasst.

a) Finalität von Transaktionen

Grundsätzlich ist die Finalität von Transaktionen im Aufsichtsrecht durch Art. 89 FinfraG geregelt. Im Zusammenhang mit DLT-Handelssystemen liesse sich aber auch argumentieren, dass die Anordnungen zur Finalität wegen der zeitlichen Verschränkung von Verpflichtungs- und Verfügungsgeschäft in Folge der DL-Technologie überflüssig seien. Unabhängig von der aufsichtsrechtlichen Finalität kommt mit der neuen Norm von Art. 973f OR auch eine zivilrechtliche Finalität zum Tragen; es gilt dabei zu beachten, dass die Regelungen von Art. 973f OR und Art. 89 Abs. 2 lit. b FinfraG nicht identisch sind.[183]

182 *EFD*, 2021, 34.

183 Zu dieser Thematik im Detail vgl. Kap. V.A.3.c)bb).

b) Anpassungen im Bucheffektengesetz

Mit der Schaffung der Registerwertrechte haben sich auch Änderungen im Bucheffektengesetz (BEG) aufgedrängt. Die Anpassungen beruhen aber eher auf den zivilrechtlichen als den aufsichtsrechtlichen Regelungen. Es sind insbesondere redaktionelle Anpassungen und Ergänzungen, um die neue Kategorie der Registerwertrechte zu erfassen. Darüber hinaus gelten neu gemäss Art. 4 Abs. 2 lit. g BEG auch DLT-Handelssysteme nach Art. 73a–73f FinfraG in Bezug auf immobilisierte Registerwerte als Verwahrungsstellen. Gemäss Art. 6 Abs. 1 lit. d BEG und Art. 6 Abs. 3 BEG können Registerwertrechte bei solchen Verwahrungsstellen zu Bucheffekten gemacht werden, wenn die Registerwertrechte im bisherigen Wertrechteregister stillgelegt werden. Die Registerwertrechte verhalten sich dann wie zentral verwahrte physische Wertpapiere und werden auch nach deren Regeln behandelt.[184]

c) Anpassungen im Nationalbankengesetz

Das Nationalbankengesetz hat eine redaktionelle Änderung erfahren. Da die DLT-Handelssysteme in Art. 2 lit. a FinfraG in den Katalog der Finanzmarktinfrastrukturen aufgenommen wurden, sind sie in Art. 19 NBG ebenfalls erwähnt. Darüber hinaus findet sich ein Hinweis auf die DLT-Handelssysteme auch in Art. 20 NBG.

D. Alternative Handelssysteme

1. Notwendigkeit alternativer Handelsplätze

Zwar enthält Art. 73f FinfraG verschiedene Erleichterungen bei den Anforderungen an kleine DLT-Handelssysteme, doch sind die Voraussetzungen für die Bewilligung, welche solche Handelssysteme bei der FINMA einzuholen haben, weiterhin hoch. Kleine Unternehmen, insbesondere Start-up-Unternehmen, dürften verbreitet nicht in der Lage sein, aus wirtschaftlichen oder administrativen Gründen die entsprechenden Anforderungen zu erfüllen. Alternative Handelsplätze «unterhalb» der vom FinfraG vorgegebenen «Schwellen» erweisen sich deshalb als notwendig.

184 Botschaft DLT-Gesetz, BBl 2020, 271 f. und 308; vgl. auch *von der Crone/Baumgartner*, 2020, 360.

In diesem Bereich ist eine gewisse Rechtsunsicherheit aber nicht zu übersehen. Aus diesem Grunde hat die Swiss Blockchain Federation einen Leitfaden 2020/1 für Unternehmen entwickelt, die sich für ein solches System interessieren. Der Leitfaden gibt insbesondere Hinweise zu den DLT-Handelssysteme und zu drei möglichen Alternativen, nämlich den dezentralen Handelssystemen, den Bulletin Boards und den durch die Emittenten organisierten Marktplätzen. Ausserdem nimmt der Leitfaden auch noch Stellung zur Liquiditätsschaffung durch Market Maker.[185]

2. Mögliche Alternativen

a) Überblick

Der Bundesrat unterscheidet in seinem DLT-Bericht zwischen vier Kategorien von DLT-Handelsplattformen. Die zentralen und dezentralen Handelsplattformen unterliegen grundsätzlich einer Bewilligungspflicht nach FinfraG. Geldwechsel-Plattformen bedürfen keiner Bewilligung, solange sie keine Verwahrungsdienstleistungen anbieten oder mit als Effekten zu qualifizierenden Token handeln. Als weitere Kategorie gibt der Bundesrat die Distributed- oder Peer-to-Peer Plattformen an, welche ebenfalls keiner Bewilligungspflicht unterstehen, und zwar unabhängig davon, ob sich die vermittelten Transaktionen auf solchen Plattformen auf Effekten beziehen oder nicht.[186] Die Botschaft deutet eine offene Haltung gegenüber weiteren, möglichen Geschäftsmodellen an.[187] In der Praxis sind beispielsweise auch Bulletin Boards, nicht-gewerbsmässige DLT-Handelssysteme und durch Emittenten organisierte Marktplätze vorstellbar.

Beim Angebot einer solchen Plattform stellt sich dennoch die Frage, welche Organisations- und Überwachungspflichten der Betreiber zu erfüllen hat.

b) Unterscheidung zwischen zentralen/dezentralen Handelsplattformen und Peer-to-Peer Handelsplattformen

Der Bundesrat hat erstmals in seinem DLT-Bericht die Unterscheidung zwischen Peer-to-Peer Handelssystemen (auch distributed Handelssysteme) und dezentralen Handelssystemen aufgegriffen.[188]

185 SBF, 2021b, 12 ff.

186 *Bundesrat*, 2018, 105 f.

187 Botschaft DLT-Gesetz, BBl 2020, 272 f.

188 *Bundesrat*, 2018, 105 f.

Diese Unterscheidung zwischen zentralen/dezentralen Systemen und Peer-to-Peer Handelssystemen ist in der Praxis von grosser Bedeutung und hat weitreichende Auswirkungen auf die rechtliche Regelung der jeweiligen Handelssysteme. Während zentrale und dezentrale Handelssysteme der Bewilligungspflicht der FINMA unterstehen, müssen die Betreiber von Peer-to-Peer Handelsplattformen keine Bewilligung einholen, ungeachtet dessen, ob sich die Transaktionen der Peer-to-Peer Plattform auf Effekten beziehen oder nicht. Trotz dieser bedeutsamen Folgen hat der Bundesrat den Begriff der Peer-to-Peer Handelsplattformen nicht definiert.[189]

In einem zentralen System sind alle Teilnehmenden mit einem zentralen Netzwerk oder einem Server verbunden; sie treffen sich alle an einem Punkt. Auf zentralen DLT-Handelssystemen haben die Teilnehmenden keinen direkten Zugriff auf die Transaktionsabwicklung und sind auf die Mitwirkung der Handelsplattformen angewiesen. Die Handelsplattform hat die Verfügungsmacht über die DLT-Effekten.[190]

In einem dezentralen System gibt es kein zentrales Netzwerk. Die Teilnehmenden haben jeweils eine eigene «Kopie» ihrer Daten und können deshalb DLT-Effekten eigenständig, ohne Mitwirkung der Handelsplattform, auf Dritte übertragen. Die Teilnehmenden «treffen sich» bloss auf der Handelsplattform, welche als Vermittlerin das Bindeglied zwischen der Käuferseite und Verkäuferseite ist. Im Gegensatz zu zentralen Systemen hat die Handelsplattform in dezentralen Systemen keine Verfügungsmacht über die DLT-Effekten, aber sie kann andere Massnahmen ergreifen, um den Angeboten auf ihrer Plattform eine bindende Wirkung zu geben. In dezentralen Systemen ist die ordnungsgemässe Ausführung der Geschäfte dank einer Reihe von Regeln – grundsätzlich vollzogen über einen Smart Contract – gewährleistet. Im Gegensatz zu Peer-to-Peer Handelssystemen bzw. distributed Handelssystemen können die Teilnehmenden auf dezentralen Systemen nicht entscheiden, mit welcher Partei ein Trade stattfindet; sie werden automatisch mit dem besten Trade zusammengebracht.[191]

189 Der Bundesrat definiert sowohl zentrale Handelsplattformen als auch dezentrale Handelsplattformen (vgl. *Bundesrat*, 2018, 146 f.); der Bericht verzichtet dabei auf die Definition der Peer-to-Peer Plattformen.

190 Vgl. hierzu Kap. III.D.2.a).

191 Vgl. auch *SBF*, 2021b, 9.

Die Peer-to-Peer Handelssysteme bzw. distributed Handelssysteme («verteilte» Handelssysteme) haben – ähnlich wie die dezentralen Systeme – kein zentrales Netzwerk. Die Peer-to-Peer Handelssysteme gehen aber einen Schritt weiter und weisen gar keine Zentralisierung auf, auch kein «Sich-Treffen» auf der Handelsplattform; sie dienen bloss für das «Informational Matching». Da nur ein Informational Matching stattfindet, können die Peer-to-Peer Handelssysteme bzw. distributed Handelssysteme eine ordnungsgemässe Ausführung der Geschäfte nicht auf dieselbe Art und Weise wie die dezentralen Systeme gewährleisten.[192] Auf Peer-to-Peer Handelssystemen bzw. distributed Handelssystemen haben die Teilnehmenden die vollumfängliche Kontrolle und Verfügungsmacht über ihre Daten. Bei der Übertragung der DLT-Effekten ist konsequenterweise keine Handelsplattform als Vermittlerin zwischengeschaltet; eine Art von «Handelsplattform» ist vielmehr vorgelagert, z.B. in Form von Bulletin Boards.

Auf der rechtlichen Ebene ist insbesondere interessant, wie viel Kontrolle die Betreibenden der Peer-to-Peer Handelssysteme bzw. distributed Handelssysteme benötigen, um rechtlich als Betreibende zu gelten. Potenziell relevante Kriterien für die Ermittlung der Qualifikation als Betreibende des Handelssystems sind, ob sie Entscheidungsgewalt darüber haben, wer zum Handelssystem Zugang hat, welche Token auf dem Handelssystem gehandelt werden und welche Aufträge miteinander zusammenzuführen sind. Falls die Betreibenden diese Kriterien nicht erfüllen, ist die Wahrscheinlichkeit klein, dass sie doch unter die Bewilligungspflicht nach FinfraG fallen. Unabhängig von dieser Qualifikation ist es wichtig, dass sie auf keinen Fall Zugang zu den gehandelten Geldern haben sollten (auch mit Hinblick auf die Bestimmungen im GwG).[193]

c) Bulletin Boards

Ein Bulletin Board erlaubt Anbietern und Käufern, für Transaktionen zu werben, ohne dass es zu einem Transaktionsabschluss kommt. Das FINMA-Rundschreiben 2018/1 «Organisierte Handelsplattformen» (OHS) legt fest, unter welchen Voraussetzungen ein OHS gemäss Art. 42 FinfraG vorliegt, und klärt, dass Bulletin Boards keine Handelssysteme sind.[194]

---

192 Vgl. auch SBF, 2021b, 9. Bei dieser Differenzierung stellt sich die Frage, welchen Nutzen Peer-to-Peer Handelssysteme bzw. distributed Handelssysteme in der Praxis haben werden, da unverbindliche Angebote in einem sehr volatilen Umfeld wenig sinnvoll sind; Wirkung entfalten solche Handelssysteme nur bei kurzfristigen Transaktionsabwicklungen.

193 *Ibid.*

194 FINMA, 2018b, Rz. 10.

Da ein Bulletin Board bloss für die Bekanntmachung von Verkaufs- und Kaufsinteressen benutzt wird, kommt es nicht zu einem Vertragsabschluss auf der entsprechenden Plattform. Dennoch (oder genau deshalb) ist von Bedeutung, dass die Regeln einheitlich ausgestaltet und für die Beteiligten auch verbindlich sind. Der Vertragsabschluss erfolgt nachgelagert im Sinne eines Peer-to-Peer Handelssystems und losgelöst von einem zentralen Netzwerk.

d) Nicht-gewerbsmässige DLT-Handelssysteme

Ein DLT-Handelssystem muss gewerbsmässig betrieben werden (Art. 73a Abs. 1 FinfraG); fehlt die Gewerbsmässigkeit, entfällt die Aufsicht, doch können andere Finanzmarktgesetze (insbesondere das GwG) zur Anwendung gelangen. Sinn dieser Regelung ist, Handelssysteme unter den Schwellen der Regulierungen für DLT-Handelssysteme von der Bewilligungspflicht auszunehmen, da diese Vorgaben für nicht-gewerbsmässig betriebene DLT-Handelssysteme unverhältnismässig sind.[195] Es ist beispielsweise denkbar, dass ein Emittent ein kleines DLT-Handelssystem für den Handel mit eigenen Aktien eröffnet und hierfür nicht denselben Bewilligungspflichten unterliegt.[196]

e) Durch Emittenten organisierte Marktplätze

Die Emission von digitalen Aktiven setzt die Einhaltung verschiedener Anforderungen voraus. Erfüllt der Emittent diese Anforderungen, bleibt es ihm unbenommen, einen anschliessenden Handel selber zu organisieren, ohne auf ein etabliertes DLT-Handelssystem zurückgreifen zu müssen.

Ein solches Vorgehen mag insbesondere in kleineren Aktiengesellschaften, deren Aktien als digitale Aktiven ausgegeben worden sind und die nicht einem sehr starken Handel unterliegen, geeignet sein. Regulatorisch darf aber bei der Zurverfügungstellung einer solchen Handelsplattform keine Gewerbsmässigkeit vorliegen. Gewerbsmässigkeit ist gemäss Art. 73a Abs. 2 FinfraG gegeben, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt. Der Bundesrat hat den Begriff in Art. 58b FinfraV weiter konkretisiert.[197]

---

195 Vgl. im Detail Kap. III.C.1.b).

196 So auch SBF, 2021b, 10.

197 Vgl. ausführlicher zu Art. 58b FinfraV Kap. III.C.1.b).

3. Governance-Anforderungen an alternative Handelssysteme

Selbst wenn eine Handelsplattform für digitale Aktiven nicht bewilligungspflichtig ist und demgemäss vom Betreiber auch keine Bewilligung bei der FINMA eingeholt wird, sind grundlegende Governance-Anforderungen, wie sie für die Betreiber von DLT-Handelssystemen gelten, zu beachten.

Zentral ist jedenfalls die Schaffung von Transparenz über die Handelsaktivitäten. Hierzu bedarf es einerseits der Aufklärung für die Teilnehmenden analog zu Art. 73e Abs. 1 FinfraG.[198] Ausserdem sollten auch regelmässig Informationen zu Handelsvolumen und Handelspreise veröffentlicht werden.

Weiter ist die Vermeidung von Risiken im Kontext der Geldwäscherei und der Terrorismusfinanzierung von Bedeutung. Weder die dezentralen Handelsplattformen noch die Peer-to-Peer Handelsplattformen verfügen über einen Private Key[199] der Kunden und haben somit keine Verfügungsmacht über die fremden Vermögenswerte. Die Abwicklung des Geschäfts erfolgt direkt auf der Blockchain zwischen den Kunden durch Smart Contracts.[200] Bei dezentralen Handelssystemen betreibt die Handelsplattform den Smart Contract und untersteht den Kontroll- und Einflussnahmemöglichkeiten der Plattform. Ermöglicht die Handelsplattform die Übertragung der Vermögenswerte durch einen von ihr betriebenen Smart Contract, wird dies bei einer weiten Auslegung der Verfügungsmacht von fremdem Vermögen als Hilfe angesehen, Vermögenswerte anzulegen oder zu übertragen (Art. 2 Abs. 3 GwG i.V.m. Art. 4 GwV).[201]

Gemäss Art. 4 Abs. 1 lit. b GwV sollen Finanzintermediäre, welche die Überweisung von virtuellen Währungen an eine Drittperson ermöglichen und eine dauernde Geschäftsbeziehung mit der Vertragspartei unterhalten, ebenfalls dem Geldwäschereigesetz unterstellt sein. Darunter fallen namentlich auch

198 Vgl. Kap. III.C.3.

199 Vgl. zu den Private Keys Kap. II.B.4.b).

200 Vgl. zu den Smart Contracts Kap. II.B.5.

201 Vgl. Botschaft DLT-Gesetz, BBl 2020, 306; *EFD*, 2021, 22, der die dezentralen Handelsplattformen ausdrücklich erwähnt; *Bundesrat*, 2018, 146 f. In Art. 2 Abs. 2 lit. d^{quater} GwG sind darüber hinaus auch die Handelssysteme für DLT-Effekten nach Art. 73a FinfraG aufgeführt.

dezentrale Handelsplattformen, welche keinen Private Key der Kunden besitzen und die Übertragung der virtuellen Währungen mittels Smart Contract abschliessen.[202]

Führt die Handelsplattform jedoch nur die Käuferinnen und Käufer mit den Verkäuferinnen und Verkäufern zusammen, wie beispielsweise auf Bulletin Boards, und wird die Abwicklung der Transaktion ohne Smart Contracts durchgeführt, stellt dies eine reine Vermittlungstätigkeit ohne Einbezug der Plattform in die Zahlungsflüsse dar. Diese Anbieter sind nicht dem GwG unterstellt.[203] Der Bundesrat ist sich dieses Risikos bewusst. Da solchen Plattformen die Verfügungsmacht fehlt, führen sie keine finanzintermediären Tätigkeiten durch. Auch die FATF hat Tätigkeiten bzgl. Kryptowährungen ihren Standards unterstellt,[204] ohne sich jedoch bisher ausdrücklich zur Anwendung dieser Standards auf die gänzlich dezentralen Handelsplattformen zu äussern; sie erwähnt bloss die Identifikation und Beurteilung der Geldwäscherei in Bezug auf neue Technologien und damit zusammenhängenden bestehenden und/oder neuen Produkten. Ausserdem unterstehen diese Plattformen auch international (noch) nicht den Regeln der Geldwäschereibestimmungen. Der Bundesrat hat dem Länderbericht der FATF über die Schweiz Rechnung getragen und in der Revision des GwG die Überprüfung der Identität der wirtschaftlich berechtigten Personen festgeschrieben.[205]

Überdies sind die Regeln zum Insiderhandel, die ggf. auch auf alternativen Handelssystemen zur Anwendung kommen können, zu beachten. Die FINMA wendet bereits heute Art. 142 FinfraG gegenüber prudentiell beaufsichtigten Marktteilnehmern gestützt auf die Gewähr einer einwandfreien Geschäftstätigkeit sinngemäss selbst in gesetzlich nicht erwähnten Märkten an.[206] Obwohl diese Anwendung langjähriger Praxis der FINMA entspricht, ist sie vom Legalitätsprinzip («nulla poena sine lege») nicht abgedeckt.[207] Das Ergebnis, dass Tätigkeiten, die nicht vom Wortlaut von Art. 142 FinfraG erfasst sind, auch sank-

202 EFD, 2021, 22. Zur Anwendung des GwG und der GwV vgl. auch *Stengel/Bianchi*, 2021.

203 *Bundesrat*, 2018, 147; *Bundesrat*, 2014, 16.

204 Vgl. The FATF Recommendations vom 16. Februar 2012 (Stand März 2022), abrufbar unter: www.fatf-gafi.org > Publications > All Publications > FATF Standards > FATF Recommendations und dort insbesondere Empfehlung 15 sowie die Erläuterungen im FATF Glossar zu «Virtual Asset» und «Virtual Asset Service Provider».

205 Botschaft GwG, BBl 2019, 5474 ff.; ferner FINMA, 2022, 9; der Bundesrat beobachtet weiterhin Risiken im Rahmen der Geldwäscherei (*Bundesrat*, 2021, 32).

206 FINMA, 2013a, Rz. 41–44.

207 FINMA, 2013b, 11 f.

tioniert werden, begründet die FINMA mit dem Gewährserfordernis und nicht mit einer extensiven Auslegung von Art. 142 FinfraG.[208] Entsprechende Überlegungen gelten auch für den Tatbestand der Kursmanipulation (Art. 143 StGB), der ebenfalls gewährsrelevant ist.

Mit dem DLT-Gesetz ist – wie erwähnt[209] – die Strafnorm von Art. 154 FinfraG zum Ausnützen von Insiderinformationen durch die Abs. 1 lit. a und lit. c sowie die Abs. 3 und 4 ergänzt bzw. erweitert worden. Handlungen auf DLT-Handelssystemen sind nun über die bisherige extensive Gesetzesauslegung zur Gewährskriterium[210] hinaus ausdrücklich strafbewehrt; für alternative Handelssysteme bleibt es hingegen beim Kriterium der einwandfreien Geschäftsführung.

4. Anhang: Liquiditätsschaffung durch Market Maker

Der Sekundärhandel lebt davon, dass ausreichende Liquidität für die Abwicklung von Handelstransaktionen vorliegt. Diese Liquidität muss nicht zwingend von den Betreibern der DLT-Handelssysteme geschaffen werden, sondern in Frage kommen auch Aktivitäten anderer Finanzmarktintermediäre. Im Vordergrund stehen die Market Maker, die ebenso im Rahmen traditioneller Handelsplätze aktiv sind.

Ein Market Maker ist in der Regel als Finanzmarktintermediär zur Einholung einer Bewilligung seitens der FINMA verpflichtet (Art. 41 FINIG). Gemäss Art. 41 lit. c FINIG gilt als Wertpapierhaus, wer gewerbsmässig und auf eigene Rechnung kurzfristig und öffentlich dauernd oder auf Anfrage Kurse für einzelne Effekten stellt.

Der Market Maker handelt gewerbsmässig, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt (Art. 3 FINIG). Kurzfristig auf eigene Rechnung handelt ein Market Maker, wenn er mit einem aktiven Anlagestil (engl. active management) in einem volatilen Marktumfeld Gewinn erwirtschaftet, und zwar unabhängig davon, ob Händler das Market Making professionell betreiben oder nicht. Die Bewilligungserteilung hat zur Folge, dass der Market Maker eine Vielzahl von in Art. 66 ff. FinfraV verankerten Pflichten zu beachten hat.[211]

---

208 BSK FinfraG-*Hoch/Hotz*, Art. 142 Rz. 24; SK FinfraG-*Sethe/Fahrländer*, Art. 142 Rz. 14; OFK FinfraG-*Vogel/Heiz/Luthiger*, Art. 142 Rz. 5 f.; *Monsch*, 2018, Rz. 729 f.

209 Vgl. Kap. III.C.5.

210 SK FinfraG-*Sethe/Fahrländer*, Art. 154 Rz. 87 ff.

211 *Schleiffer/Schärli*, 2018, § 22 N 158.

Wie erwähnt, kann das Market Making dem Emittenten überlassen werden, wenn nur dessen Aktien gehandelt werden.[212] Der Vorteil dabei wäre, dass aus buchhalterischer Sicht das Bestandsrisiko wegfällt, da ein Kapitalgewinn und -verlust der eigenen Aktien nach den internationalen Regeln der Buchhaltung nicht verrechnet wird. Dennoch ist jegliche Market Making Aktivität durch den Emittenten transparent zu halten; durch den Einsatz von Smart Contracts liesse sich auch die Gefahr des Insiderhandels minimieren.

E. Einsatz von Algorithmen in (DLT-)Handelstransaktionen

Mit der zunehmenden Popularität der DLT-Handelstransaktionen stellt sich die Frage, welche Rolle der Einsatz von Algorithmen in diesem Umfeld spielen wird. Beim Einsatz von Algorithmen ist insbesondere der Hochfrequenz-Handel ein Problembereich, da nicht klar ist, ob die Vor- und Nachhandelstransparenz noch angemessen funktioniert. Die potenziell hohe Handelsliquidität im Bereich der DLT wirkt geradezu einladend für einen noch effizienteren Einsatz von Algorithmen in DLT-Handelstransaktionen. Damit es nicht zu einer ausufernden Verwendung von Algorithmen kommt, ist es wichtig, dass die entsprechenden Vorgaben zu KYC und AML auch auf DLT-Handelssystemen eingehalten werden.

Nachfolgend wird zunächst überblicksweise die Entwicklung des algorithmischen Handels an den Finanzmärkten dargestellt (1.) und deren Regulierung in der EU und der Schweiz beschrieben (2.). Danach wird erklärt, wie der Einsatz von Algorithmen in Märkten von Krypto-Assets funktioniert (3.) und welche regulatorischen Vorgaben für den Handel auf DLT-Handelsplätzen erforderlich sind (4.). Schliesslich ist kurz auf die künftigen Entwicklungen einzugehen (5.).

212 Falls Emittenten das Market Making übernehmen, sollte diese Tätigkeit als nicht profitables, eigenständiges Geschäft organisiert werden (vgl. SBF, 2021a, 10 f.).

1. Entwicklung des algorithmischen Handels an den Finanzmärkten

a) Computerisierung

Die Zeiten von Börsenmaklern auf dem Parkett sind schon lange vorbei. Bereits seit Jahren haben Computer geholfen, die Orderflut zu lenken, d.h. dank des computerisierten Handels ist es einfacher geworden, Kauf- und Verkaufsorders zu «matchen». Der technische Fortschritt prägte den Strukturwandel und der elektronische Handel hat das «Börsenparkett» verdrängt.

Die globalen Finanzmärkte und ihre Handelsplattformen sind in den vergangenen Jahren laufend weiter optimiert und automatisiert worden.[213] Abgesehen vom Vergleich der Kosten und Preise gilt es, unter Berücksichtigung der Ausführungsqualität die Aufträge an den bestmöglichen Handelsplatz zu bringen (engl. best execution). Im Rahmen der Marktliberalisierung etablierten sich deshalb neben den traditionellen Börsen vermehrt Handelssysteme, die es Finanzintermediären ermöglichen, die Transaktionskosten zu senken.[214]

b) Algo- und High Frequency Trading

Nicht nur die Handelsplätze selbst wurden automatisiert, sondern auch die Aufbereitung der Orderflut erfolgt computerisiert. Dies ermöglicht es Market Makern, Hedge Funds und anderen institutionellen Investoren, neue Geschäftsmodelle zu entwickeln. Der computergestützte Handel setzt heute Algorithmen ein, um die Informationsbeschaffung und -verarbeitung durch die permanente Beobachtung und Analyse von Marktdaten zu optimieren. Unter der Bezeichnung «automatisierter» oder «algorithmischer Handel» ist der automatische Handel von Wertpapieren durch Computerprogramme an einem Marktplatz zu verstehen.

Auf Basis von vorhandenen und aufbereiteten Daten lassen sich automatisierte Kauf- und Verkaufsaufträge (sog. Orders) an den jeweils vorteilhaftesten Handelsplatz (engl. order routing) schicken. Die menschliche Einbindung beschränkt sich auf die Programmierung der verwendeten Codes.[215] Neben der

213 Vgl. *Zimmermann*, 2012, 97 ff.

214 Die in den USA zulässige Möglichkeit, insbesondere Online-Broker dafür zu bezahlen, dass diese die Orders ihrer Privatanleger an grosse Händler zur Abwicklung übergeben, führt für den Kleinanleger zu einem Wegfall der abgerechneten Transaktionskosten.

215 Vgl. *Contratto*, 2014, 145.

Entscheidung darüber, welche Menge und welchen Preis eine Order beinhaltet, erlauben bestimmte Marktplätze eine Vielzahl von durchzuführenden Order-Varianten. Von Hochfrequenz-Handel (engl. High Frequency Trading, HFT) wird dann gesprochen, wenn der algorithmische Handel zum Teil in Millisekunden zur Abwicklung gelangt. Die MiFID-II-Richtlinie versteht HFT als Subkategorie zum algorithmischen Handel.[216]

Neben einer technisch optimierten Infrastruktur zur Vermeidung von Zeitverzögerungen bei der Ausführung der Aufträge ist eine nicht gerade billige, sehr enge Anbindung an die Computerinfrastruktur des Marktplatzbetreibers erforderlich, um die durch die Datenleitung bedingte Zeitverzögerung zu minimieren. Dazu positioniert sich der Händler möglichst «nah» am Handelsplatz, um bei bestmöglicher Dateninfrastruktur und Rechenleistung schneller als andere Marktteilnehmende zu agieren; für diesen bevorzugten Zugang (engl. Co-Location) erheben die Marktplätze entsprechende Gebühren.

Im Prinzip nutzt der auf Algorithmen basierende Handel vorhandene Marktpreisineffizienzen aus; in volatilen Märkten ist der Einsatz von Algorithmen besonders lukrativ. Diese Prämisse der Volatilität wird von den Krypto-Märkten zweifellos erfüllt. Allerdings setzt die erfolgreiche Anwendung von Algorithmen auch voraus, dass diese auf Vergangenheitswerten basierende Strategien berücksichtigen; der noch junge Krypto-Handel bietet hierzu indessen noch wenig Datenmaterial.

c) Einsatz von künstlicher Intelligenz

Entwicklungen im Bereich des maschinellen Lernens und der Einsatz von künstlicher Intelligenz (KI) beeinflussen auch die Programmierung im Bereich des algorithmischen Handels an den Finanzmärkten. Unter «KI» wird in der Regel die Entwicklung und der spätere Einsatz von Computersystemen verstanden, mit deren Hilfe menschliche Intelligenz ersetzt wird. Beim Algo-Trading geht es vornehmlich um Entscheidungsfindungsprozesse; deshalb kann im Prinzip bereits das automatisierte Auslösen einer Order beim Erreichen eines bestimmten Kurses unter den Begriff «KI» fallen.

216 MiFID-II-Richtlinie Art. 17 Abs. 1 und 2.

Schon in den Anfängen beruhte dieser Handel auf hochentwickelten Formen der Datenverarbeitung; so entstand auch der Begriff der «Quants»,[217] welche die Szene dominierten. Generell geht es beim Hochfrequenzhandel (HFT) aber vor allem um Geschwindigkeit und grosse Volumina, so dass der Einfluss von hochentwickelten KI-Modellen nicht überschätzt werden darf. Allerdings kommen zwischenzeitlich neben den eher einfachen HFT-Algorithmen vermehrt komplexere Algorithmen zum Einsatz, die nicht nur interne Daten verarbeiten, sondern auch soziale Daten und Stimmungsanalysen berücksichtigen.

d) Unterscheidung zwischen Ausführungs- und Entscheidungs-Algorithmen

Während Algorithmen für Anlageentscheidungen automatisierte Handelsentscheidungen treffen, indem sie bestimmen, welches Finanzinstrument gekauft oder verkauft werden soll, optimieren Orderausführungsalgorithmen die Orderausführungsprozesse durch automatische Generierung und Übermittlung von Orders oder Kursofferten an einen oder mehrere Handelsplätze, nachdem die Anlageentscheidung selbst schon getroffen wurde.

Weil Handelsalgorithmen lediglich Anlageentscheidungen treffen, erweisen sich geringere regulatorische Vorgaben als erforderlich. Bei Auftragsausführungsalgorithmen sind die potenziellen Auswirkungen auf das faire und ordnungsgemässe Funktionieren des Marktes zu analysieren. Deshalb hat die EU (RTS 2017/589) spezielle Anforderungen an Tests für Handelsalgorithmen eingeführt, um Auswirkungen dieser Algorithmen auf das Funktionieren des Markts zu untersuchen.[218]

---

217 Quant ist eine Abkürzung für «Quantitative Analyst», d.h. Analysten, die mit den Methoden der Mathematik und Statistik komplexe Finanzstrategien entwickeln, die im Bereich statistische Arbitrage, algorithmischer Handel oder auch beim elektronischen Market Making Einsatz finden; vgl. dazu *Patterson*, 2010, und *Patterson*, 2012.

218 Vgl. Erwägung (5) der Delegierte Verordnung 2017/589 vom 19. Juli 2016 zur Ergänzung der Richtlinie 2014/65 durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Wertpapierfirmen, die algorithmischen Handel betreiben, ABl. L 87, 417–448 (RTS 2017/589).

e) Auswirkungen des Hochfrequenzhandels

Einerseits kann der HFT in den Finanzmärkten bestehende potenzielle Vorteile effizienter machen, weil mehr Liquidität im Markt vorhanden ist und sich eine verbesserte Preiseffizienz ergeben kann, womit sich letztlich engere Geld-Brief-Spannen und niedrigere Transaktionskosten ergeben. Andererseits führt HFT durch die massiv erhöhte Handels-Geschwindigkeit dazu, dass Preisschocks schneller durchschlagen und gegebenenfalls Volatilität in übertriebener Form generieren, was zu systemischen Risiken führt (Flash Crash). Ein schneller Rückgang des Kurses eines Wertpapiers durch automatisierte Handelstools vermag sich auch auf gesamte Indizes und Märkte auszuwirken.

Ein weiterer wichtiger Kritikpunkt an HFT besteht darin, dass die positiven Liquiditätseffekte in Krisenzeiten durch das Aussetzen des algorithmischen Handels den Markt völlig austrocknen. Dies erweist sich als problematisch, weil Liquidität gerade in einer Krise wichtig ist.

2. Regulierung des algorithmischen Handels an den Finanzmärkten

a) Regulatorische Herausforderungen

Systemimmanente Trade-offs durch die technische Komplexität auf Handels- und Order-Ebene verbunden mit der komplexen IT-Infrastruktur sind regulatorisch so zu erfassen, dass ein stabiles und transparentes Handelsgeschehen gewährleistet wird.[219] Allerdings führt der in Millisekunden abgewickelte Handel dazu, dass den regulatorischen Anforderungen erst im Rahmen der Nachhandelstransparenz Genüge getan werden kann.

Effizient funktionierende Kapitalmärkte setzen einen gut regulierten Informationsfluss (Vor- und Nachhandelstransparenz) zwischen allen Beteiligten voraus, um etwaige Missbräuche einzudämmen bzw. deren Aufdeckung zu ermöglichen.[220] Unter anderem zur Ausführung grosser Orders erlaubt aber der Regulator oft Ausnahmen bei der Handels-Transparenz, was als «Dark Trading» bezeichnet wird.[221]

---

219 Vgl. *Hertig*, 2012.

220 Vgl. *Alexander*, 2012. 34; generell erschweren Dark Pools die Aufdeckung von Insider Dealing und Marktmanipulation.

221 Vgl. dazu *Baisch/Baumann/Weber*, 2014, passim.

b) Vor- und Nachhandelstransparenz

In der EU enthielt die Wertpapierrichtlinie 93/22/EWG in Art. 21 lediglich Transparenzvorschriften für geregelte Märkte, d.h. für die national streng regulierten Börsen.[222] Die MiFID-Regulierung führte zu einem stärkeren Wettbewerb zwischen den Finanzdienstleistern, weil Multilaterale Handelssysteme (engl. Multilateral Trading Facility, MTF) den klassischen Börsen Konkurrenz machten. Wie MiFID und MiFIR in der EU[223] enthalten auch FinfraG und FinfraV konkrete Regeln zur Vor- und Nachhandelstransparenz (Art. 29/46 FinfraG, Art. 27-29, 42-43 FinfraV); allerdings kennen MiFID und MiFIR deutlich detailliertere Ausnahmebestimmungen, die festlegen, in welchen Fällen die Aufsichtsbehörden in den Mitgliedstaaten auf die Vorhandelstransparenz verzichten können.

Unter Vorhandelstransparenz ist die Information der Marktteilnehmenden über die aktuelle Auftragslage an einem bestimmten Handelsplatz zu verstehen (Art. 29 Abs. 1 und 3 lit. a FinfraG, Art. 27 FinfraV). In der Praxis wird diese Transparenz durch ein heute digital einsehbares Auftragsbuch des Handelsplatzes gewährleistet, in dem die aktuellen Geld- und Briefkurse mit den entsprechenden Order-Volumina publiziert werden. Bei engeren Märkten dienen die Kursofferten von Market Makern dem gleichen Zweck.[224]

Die Nachhandelstransparenz verpflichtet zur Veröffentlichung von Nachhandelsinformationen (insbesondere Preis und Volumen), der Handelsplatz hat also über alle abgeschlossenen Transaktionen zu berichten (Art. 29 Abs. 2 und 3 lit. b, FinfraG, Art. 28 FinfraV).

222 Vgl. zum Übergang von der Wertpapierrichtlinie zur MiFID: *Maurenbrecher*, 2005, 35.

223 Eine solche Waiver-Bestimmung kann z.B. eine *Large-in-Scale-Transaction* betreffen.

224 Bilaterale OHS können die Anforderungen der Vorhandelstransparenz durch die Veröffentlichung von verbindlichen Angeboten erfüllen. Falls für ein bestimmtes Finanzinstrument kein liquider Markt gegeben ist, genügen Kursofferten auf Anfrage; vgl. FINMA-Rundschreiben 2018/1: Organisierte Handelssysteme – Pflichten von Betreibern eines organisierten Handelssystems (OHS), N 37.

c) EU-Regulierungen in MiFID/MiFIR/MiCA

Viele Krypto-Assets sind wohl gemäss MiFID als Finanzinstrumente zu qualifizieren, so dass die relativ strengen Regeln für Handelsplätze gemäss MiFID/MiFiR[225] Anwendung finden.[226] In der MiFID-Erläuterung (62) wird ausgeführt, dass technische Fortschritte den Hochfrequenzhandel und die Weiterentwicklung von Geschäftsmodellen ermöglichen und der Hochfrequenzhandel dadurch erleichtert wird, dass Marktteilnehmende ihre Systeme gemeinsam in unmittelbarer räumlicher Nähe zu einer Matching-Maschine eines Handelsplatzes unterbringen (Co-Location). Zudem wird auf potenzielle Risiken dieser Handelstechnologien und insbesondere auf bestimmte, gemäss Marktmissbrauchsverordnung 596/2014 verbotene «Verhaltensformen» hingewiesen.

Art. 4(1) Nr. 39 definiert den algorithmischen Handel als «*Handel mit einem Finanzinstrument, bei dem ein Computeralgorithmus die einzelnen Auftragsparameter automatisch bestimmt, z. B. ob der Auftrag eingeleitet werden soll, Zeitpunkt, Preis bzw. Quantität des Auftrags oder wie der Auftrag nach seiner Einreichung mit eingeschränkter oder gar keiner menschlichen Beteiligung bearbeitet werden soll, unter Ausschluss von Systemen, die nur zur Weiterleitung von Aufträgen zu einem oder mehreren Handelsplätzen, zur Bearbeitung von Aufträgen ohne Bestimmung von Auftragsparametern, zur Bestätigung von Aufträgen oder zur Nachhandelsbearbeitung ausgeführter Aufträge verwendet werden*»; weitere Details sind der Delegierten Verordnung zu entnehmen.[227]

Weiterführend (Art. 4(1) Nr. 40) ist eine hochfrequente, algorithmische Handelstechnik dadurch gekennzeichnet, dass eine Infrastruktur zur Minimierung von Verzögerungen (Netzwerk-Latenzen) bei der Orderübertragung Anwendung findet und ohne menschliche Intervention ein hohes untertägiges Auftragsvolumen generiert wird. Ein besonderes Merkmal ist der direkte elektro-

---

225 *MiFID*: Richtlinie 2014/65 vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92 und 2011/61, *ABl. L 173*, 349–496; *MiFIR*: Verordnung 600/2014 vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung 648/2012, *ABl. L 173*, 84–148.

226 Vgl. dazu *Baisch/Weber*, 2021, 221 ff.; *Baisch/Weber*, 2022, 173 ff.

227 Art. 18 der Delegierten Verordnung 2017/565 vom 25. April 2016 zur Ergänzung der Richtlinie 2014/65 in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie, *ABl. L 87*, 1–83.

nische Zugang dieser Handelsteilnehmer, der die Nutzung des Handelscodes gestattet, um Aufträge elektronisch direkt an den Handelsplatz zu übermitteln (Art. 4(1) Nr. 41).

Neben dem Potential für Marktmissbrauch und -manipulation kann algorithmischer Handel auch Handelssysteme überlasten und auf Marktereignisse in einer Form reagieren, dass wegen Kaskadeneffekten die Volatilität massiv erhöht wird; mittlerweile sorgen in der Regel Circuit Breaker dafür, dass bei z.B. 10%-igen Schwankungen der Handel bei einem Finanzinstrument unterbrochen wird, um computergenerierte Flash Crashes zu vermeiden.

Vor allem mit Bezug auf die nicht unbegründeten Befürchtungen bezüglich der «Stabilität» von Stablecoins plant die EU entsprechende regulatorische Vorgaben im Rahmen der MiCA (Markets in Crypto-Assets).[228] Der Kollaps verschiedener Stablecoins hat gezeigt, dass nur tatsächlich gedeckte Token eine ausreichende Werthaltigkeit gewährleisten.[229]

Vergleichbar zu traditionellen Finanzmarkt-Vorgaben untersagt Art. 68 der MiCA-Verordnung in Abs. 3 den Eigenhandel; Abs. 5 soll Anbieter von Krypto-Dienstleistungen dazu verpflichten, über alle Geld- und Briefkurse sowie die Tiefe der Handelsinteressen zu diesen Preisen während der Handelszeiten kontinuierlich öffentlich zu informieren.[230] Titel VI des MiCA-Verordnung thematisiert den Marktmissbrauch.

d) CH-Regulierungen in FinfraG/FinfraV

Art. 31 Abs. 1 FinfraV verpflichtet einen «Handelsplatz» lediglich dazu, die durch den algorithmischen Handel erzeugten Aufträge, die dabei verwendeten Algorithmen und die dafür verantwortlichen Händler zu erkennen. Hierzu ver-

228 Vgl. *Zetzsche/Annunziata/Arner/Buckley*, 2021.

229 Vgl. hierzu Kap. II.C.3.b) mit Fn. 77.

230 Vgl. auch Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM/2020/593 final, aufrufbar unter <https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0022.02/DOC_1&format=PDF>. Der Trilog zwischen den gesetzgebenden Organen ist bereits abgeschlossen; der Europäische Rat und das Europäische Parlament müssen die MiCA nur noch formal annehmen (vgl. Rat der EU, Digitalisierung des Finanzwesens: Einigung über die europäische Verordnung über Kryptowerte (MiCA) – Pressemitteilung vom 30.06.2022, aufrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.

ankert Abs. 2 eine Melde- und eine auftragsbezogene Kennzeichnungspflicht; zudem bestehen Verpflichtungen bezüglich Dokumentation und Risikokontrolle.[231] Zusätzlich verhindern die strengen von der FINMA anzuwendenden Zulassungsregeln den Markteintritt unseriöser Anbieter.

3. Algorithmischer Handel an Märkten für Krypto-Assets

a) Besonderheiten

Da Hochfrequenzhändlerinnen und -händler von der Diskrepanz zwischen Geld- und Briefkursen profitieren, indem sie die Latenz nutzen, um Vermögenswerte in Mikrosekunden zu kaufen und zu verkaufen, stellt sich die Frage, inwieweit sich die Krypto-Marktplätze für diese Techniken eignen. Die typischen vier HFT-Strategien, nämlich Market Making, Momentum Trading, Liquiditätserkennung und Arbitrage, können grundsätzlich auch bei grösseren Krypto-Assets an entsprechend liquiden Märkten Anwendung finden. Insbesondere Momentum-Strategien zur Ausnutzung kurzfristiger Preisschwankungen erscheinen erfolgsversprechend, wenn es gelingt, Marktreaktionen zu prognostizieren. Die Idee, auf die Marktaktivität anderer Händlerinnen und Händler abzustellen (Liquiditätserkennung), funktioniert nur, wenn viele andere Händlerinnen und Händler aktiv sind; dies setzt voraus, dass institutionelle Anleger am Krypto-Markt tätig werden.

Die grössten HFT-Volumina bewegen sich im Arbitrage-Handel, der Preisunterschiede zwischen Handelsplätzen gewinnbringend nutzt. Die Volatilität des Kryptowährungsmarktes macht diesen Handel zu einem verlockenden Ziel für automatisierte Transaktionen; zudem ist der Kryptowährungsmarkt vergleichbar zum Devisenmarkt 24/7 aktiv und dort nimmt der Hochfrequenzhandel eine wichtige Rolle ein. Die Ausnutzung von Geschwindigkeitsvorteilen im Mikrosekundenbereich setzt voraus, dass der Marktplatz eine entsprechende Handelsgeschwindigkeit ermöglicht. Die programmierte On-Chain-Natur ist beim Clearing und Settlement zu berücksichtigen. Weil die traditionell getrennten Dienstleistungen rund um eine Transaktion im DeFi-Sektor häufig von der gleichen Partei abgewickelt werden, erfordert dies entsprechendes Vertrauen in die Zuverlässigkeit der Plattform.

[231] Ausführlich zum Hochfrequenzhandel *Monsch*, 2018, passim.

In den letzten Jahren hat zunächst vor allem Bitcoin als Investitionsoption erhebliche Aufmerksamkeit erhalten, obwohl die Volatilität finanzielle Risiken birgt. Empirische Analyse-Tools für die Bitcoin-Prognose können aber nicht auf jahrzehntealte Datenvolumina zurückgreifen. Allerdings wird nun versucht, entsprechende Modelle zu entwickeln.[232]

b) Trading-Bots

Weil der Handel mit Kryptowährungen nie stoppt, sind Marktschwankungen permanent zu verfolgen, was den Einsatz automatisierter Systeme erfordert. Vielfach kommen dabei Krypto-Trading-Bots zum Einsatz, d.h. automatisierte Programme, die über das Internet am Handel teilnehmen und auch von privaten Anlegerinnen und Anlegern genutzt werden. Selbst Kleinanlegerinnen und -anleger haben die Möglichkeit, Tools oder Hilfen zur Erstellung eigener Programme zu kaufen, die versprechen, auch über Nacht «emotionslos» Gewinne zu generieren. Der Umstand, dass es weder Beschränkungen bei der Handelszeit gibt noch klassische «Gatekeeper» zwischengeschaltet sind, ermöglicht solche Anwendungen. Selbstverständlich setzt dies voraus, dass nicht nur die Token bei einer entsprechenden Handelsplattform verwahrt sind, sondern auch die Verfügungsgewalt an den Bot delegiert wird; dies birgt natürlich entsprechende Gegenpartei- und Cyber-Risiken.[233]

Volatilität und Risiken auf 24/7-operierenden Kryptowährungsmärkten lassen es für private Investoren als interessant erscheinen, trotz eigener Schlafphasen auf Marktbewegungen durch Handelsbots rund um die Uhr zu reagieren; zudem kann ein Kryptowährungs-Trading-Bot die Handelstransaktionen viel schneller und effizienter abwickeln, als es ein Trader selbst zu tun vermag. Mittlerweile sind zahlreiche Kryptowährungs-Trading-Bots verfügbar; einige dieser Bots sind kostenlos und Open Source, für andere sind monatliche bzw. jährliche oder transaktionsbezogene Gebühren zu entrichten.

Im Prinzip beruhen Kryptowährungs-Trading-Bots auf Softwareprogrammen, die über eine Schnittstelle (engl. Application Programming Interface, API) direkt mit den Marktplätzen verbunden sind. So bleiben die relevanten Informationen permanent verfügbar und können gemäss hinterlegten Programmvorgaben automatisch Kauf- oder Verkaufsorders generieren.

---

232 Vgl. *Li/Jiang/Li/Wang*, 2022.

233 Vgl. zur Cybersicherheit auf dem Finanzmarkt *Weber/Yildiz*, 2022; zur Cybersicherheit auf DLT-Handelsplattformen, vgl. Kap. IV.

Während Trading-Bots für die traditionellen Wertpapiermärkte sehr teuer und für den private Anleger nicht ohne Weiteres zugänglich sind, bieten Kryptowährungsbörsen ihren Benutzern direkten Zugang zu ihrem Markt und ihrem Börsenauftragsbuch. Dies ermöglicht die einfache und kostengünstige Verwendung eines Trading-Bot; im Internet kursieren auch zahlreiche Anleitungen, ein solches Programm selbst zu erstellen. Dabei geht es nicht immer um komplexe Handelsstrategien, sondern z.B. um Stop-Loss-Orders oder limitierte Verkaufs- oder Kaufaufträge, die bei der Unterschreitung eines festgelegten Kursniveaus ausgelöst werden. Aber auch eine Ausrichtung auf «Kauf-/Verkaufssignale», «Portfolio-Rebalancing» oder andere typische Algo-Trading-Optionen sind denkbar.

4. Regulierung des algorithmischen Handels an DLT-Handelsplätzen

a) Akteurinnen und Akteure

Das Financial Stability Board (FSB) und die Zentralbanken sowie die EU tendieren im Prinzip dazu, den Handel mit Krypto-Assets vergleichbar zum Handel mit bisher bekannten Finanzinstrumenten zu regulieren. Mit MiCA in der EU und wohl auch an anderen wichtigen, den FSB-Empfehlungen folgenden Finanzmarktzentren kann davon ausgegangen werden, dass ab 2023/24 Handelsplätze entsprechende Lizensierungsauflagen zu erfüllen haben; somit ergeben sich Verpflichtungen im Bereich KYC (engl. know your customer) und AML (engl. anti money launderng) sowie im Bereich Reporting. Dies wird wohl zur Folge haben, dass auch die Vorgaben zu Algo-Trading und HFT Anwendung finden dürften.

Bei Algo-Tools für private Marktteilnehmende ist derzeit nicht zu erwarten, dass der Regulator aktiv wird. Die Anforderungen an die Krypto-Handelsplätze dürften aber steigen, weshalb in Zukunft ein grösserer Beitrag zu Anlegerschutz und Finanzstabilität zu erwarten ist.

b) Potenzielle Probleme

Der absehbare Verzicht auf das Drei-Silo-Prinzip, der den Handel, die Abwicklung und die Clearing- & Settlement-Prozesse trennt, birgt Konzentrationsrisiken. Solange Eigenhandel nicht untersagt ist, können die Krypto-Handelsplätze typische HFT-Handelsstrategien selbst anwenden. Dies schliesst gewisse Formen von Marktmanipulation nicht aus. Offene Orderbücher, trans-

parentes Market Making sowie die Publikation aller Trades sollten für ein Maximum an Vor- und Nachhandelstransparenz[234] sorgen, um diese Risiken zu begrenzen.

c) Regulierungsbedarf

Die genannten Probleme zeigen den Regulierungsbedarf auf, der von den meisten Regulatoren auch erkannt worden ist. Vieles befindet sich bereits im Umbruch. Wichtig erscheint insbesondere, die Aufsichtsbehörden zu befähigen, die geplanten Massnahmen auch effektiv umsetzen zu können.[235]

5. Künftige Entwicklungen

Wie in anderen Bereichen ist mit Blick auf die Relevanz von bestehenden Regulierungen für den algorithmischen Handel von entscheidender Bedeutung, dass die Anwendbarkeit geltender Vorschriften auch für den Krypto-Sektor geklärt wird, selbst wenn die häufig hybride Natur von Krypto-Assets zu Herausforderungen führt.[236] Derzeit ist eine zunehmende Fragmentierung zu beobachten, bei der sogar bei Privaten gewisse Algo-Strategien im Rahmen des Handels mit Krypto-Assets Anwendung finden.

Einerseits gilt es somit klarzustellen, welche Krypto-Assets in den Anwendungsbereich der bestehenden Finanzdienstleistungsgesetzgebung fallen und damit der aufsichtsrechtlichen Durchsetzung unterliegen; andererseits sind durch gezielte Änderungen der bestehenden Regulierungen vorhandene Lücken zu schliessen. Nachdem zunächst die Risiken unsicherer Marktplätze und Verwahrer die Token-Anleger betrafen und bei der Ausgabe von Krypto-As-

234 Ausführlich dazu *Humbel*, 2019.

235 Zum Regulierungsbedarf im Rahmen der Cybersicherheit auf dem Finanzmarkt im Allgemeinen, vgl. *Weber/Yildiz*, 2022, 97 ff.; zu den regulatorischen Herausforderungen und den erforderlichen Massnahmen für DLT-Handelsplattformen, vgl. Kap. IV.C.

236 Vgl. *Saulnier/ Giustacchini*, 2020.

sets viele «Anlegerinnen und Anleger» verschiedenen Betrugsrisiken ausgesetzt waren,[237] wird es nach einer weiteren Marktbereinigung darum gehen, stabile und zuverlässige Handelsinfrastrukturen zu gewährleisten.[238]

Der regulatorische Perimeter ist so zu gestalten, dass Krypto-Asset-Emittenten sowie Handelsplattformen und Wallet-Anbieterinnen und -anbieter einen angemessenen Anlegerschutz sicherstellen. Eine sachgerechte Marktintegrität setzt voraus, dass eine umfassende Offenlegung der Schlüsselinformationen zu den betreffenden Krypto-Assets und aufsichtsrechtlich klare Governance-Anforderungen vorgesehen sind. Die Compliance-Vorgaben gilt es zu verbessern, um die Einhaltung von Vorschriften sowie deren Überwachung zu gewährleisten und letztlich Durchsetzungsmechanismen zu etablieren, um schädliche Folgen von Informationsasymmetrien zu verringern und Marktmissbrauch zu verhindern. Ohne sachentsprechende Lizenzierungsverfahren für die Krypto-Dienstleister und entsprechendes Knowhow bei den Aufsichtsbehörden sind diese Ziele kaum zu erreichen.[239]

237 Vgl. dazu *Zetzsche/Buckley/Arner/Föhr*, 2019; *Weber/Baisch*, 2019a; *Weber/Baisch*, 2019b.

238 Auch nach einer Beruhigung sind die Schäden immens; vgl. Federal Trade Comission, New Analysis Finds Consumers Reported Losing More than Billion in Cryptocurrency to Scams since 2021, Juni 2022; <https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021?utm_source=govdelivery>.

239 Vgl. zur Notwendigkeit passender Governance-Mechanismen *Weber/Yildiz*, 2022, 106 ff.; zum Situationsbewusstsein und zur Bedeutung der stetigen Weiterentwicklung, vgl. *Weber/Yildiz*, 2022, 111 f. und 129 f.; zu den zu beachtenden Gefahren im Rahmen der DLT-Handelsplattformen, vgl. Kap. IV.B.

IV. Resilienz und Systemstabilität von DLT-Handelsplattformen

Um die Dynamik rund um Cybergefahren für DLT-basierte Systeme zu verstehen, sind zunächst die Grundlagen der Resilienz und Systemstabilität zu erläutern (Kap. A.). In einem nächsten Schritt ist die Sicherheit und Resilienz auf DLT-Handelsplattformen zu untersuchen und auf die unterschiedlichen Angriffsmöglichkeiten einzugehen (Kap. B.). Gestützt auf diese Erkenntnisse lassen sich die regulatorischen Herausforderungen und potenziellen Massnahmen im Rahmen der DLT-Handelsplattformen diskutieren (Kap. C.).[240]

A. Grundlagen

1. Einleitung

Die DLT sollte – gemäss den zugrundeliegenden technologischen Besonderheiten – eine allgemein höhere Sicherheit aufweisen und manipulationssicher sein;[241] dennoch sind auch bei der DLT gewisse Schwachstellen erkennbar. Einerseits können einzelne Aspekte der DLT weiterhin mittels konventioneller Angriffe bedroht sein, z.B. aufgrund von Fehlern im Code, von Angriffen auf die User Interfaces[242] (dt. Benutzeroberflächen) oder Angriffen auf Private Keys bzw. von Diebstahl der Private Keys.[243] Andererseits haben sich die DLT-Handelsplattformen auf DLT-spezifische Angriffe vorzubereiten, insbesondere die 51%-Angriffe (also Consensus Hijacks [Konsens-Bevollmächtigungen]) und die Sybil-Angriffe.

Den neuen Besonderheiten und Herausforderungen im Kontext der DLT ist angemessen Rechnung zu tragen. Dies wird mit Blick auf die bereits erfolgten Angriffe ersichtlich: Im Rahmen des sog. «DAO-Hacks» konnten Angreifende

---

240 Der nachfolgende Text basiert in den Grundzügen auf *Rolf H. Weber*, Sicherheit und Resilienz in DLT-basierten Finanzmarktinfrastrukturen. In: Jusletter 13. Juni 2022 (*Weber*, 2022b); dieser Beitrag wird nachfolgend nicht weiter referenziert.

241 Vgl. zur höheren Sicherheit auf DLT-Systemen Kap. II.B.1. und II.B.3.a); vgl. zur Manipulationssicherheit Kap. II.A.2. und II.B.3.a).

242 Zur Sicherheit der User Interfaces und zu allgemeinen Angriffsmöglichkeiten auf die User Interfaces vgl. *Malisa*, 2017.

243 Vgl. zur Bedeutung der Private Keys und deren Sicherungsmöglichkeiten Kap. II.B.4.

im Jahre 2016 durch Ausnutzung eines «Loophole» ca. 12 Millionen Ether (ETH) zum damaligen Wert von über CHF 55 Mio. stehlen.[244] Im Jahre 2021 gelang es einem Hacker mit einem Angriff auf die DeFi-Plattform[245] Poly Network, über CHF 550 Mio. in Kryptowährungen zu entwenden.[246] Ein weiteres Beispiel ist der Angriff auf das Ronin Network, bei dem grossflächig Private Keys gestohlen wurden, was zur Entwendung von Kryptowährungen im damaligen Wert von ca. CHF 580 Mio. führte.[247]

2. Begrifflichkeiten

a) Sicherheit

Wie die vorgenannten Beispiele zeigen, kommt der Sicherheit im Rahmen der DLT grosse Bedeutung zu. In diesem Zusammenhang ist insbesondere der Begriff der Cybersicherheit (bzw. Cybersecurity) von Interesse.[248] Die Cybersicherheit hat weder im deutschen noch im englischen Sprachgebrauch eine einheitliche Definition gefunden; der Begriff wird vielmehr als Schlagwort verwendet, um das Sicherheitsbedürfnis im Zeitalter des Internets aufzuzeigen.[249]

---

244 *Meier/Schuppli*, 2019, 32 ff.

245 Eine DeFi-Plattform ist eine sog. Cross-Chain Decentralized Finance Platform. Solche Plattformen beruhen auf Smart Contracts und dezentralisierten, Blockchain-basierten autonomen Organisationen. Die Cross-Chain DeFi-Plattformen bieten eine Cross-Chain-Architektur (eine Architektur, die zwischen verschiedenen Blockchains funktionsfähig ist) an. Diese Architektur erleichtert die Interoperabilität, indem sie zwei oder mehr Blockchains in die Lage versetzt, ihre Dezentralisierung, ihren Funktionsumfang und ihre Sicherheit miteinander in Einklang zu bringen (vgl. auch *Weber*, 2022a, 3 ff.).

246 *Daniel Meier*, Keine Waffe, kein Sprengstoff, kein Fluchtauto: Wie ein Hacker über 610 Millionen Dollar stehlen konnte, NZZaS vom 29.08.2021, aufrufbar unter <https://nzzas.nzz.ch/hintergrund/ein-hacker-und-der-groesste-diebstahl-der-geschichte-ld.1642710>; *Gertrude Chavez-Dreyfuss/Michelle Price*, Explainer: How hackers stole and returned $ 600 mln in tokens from Poly Network vom 13. August 2021, aufrufbar unter <https://www.reuters.com/technology/white-hat-hacker-has-returned-nearly-all-600-million-crypto-tokens-taken-tuesday-2021-08-12/>.

247 Vgl. *Muyao Shen*, Hacker Moves Crypto Stolen From Ronin Breach to Help Cover Its Tracks vom 4. April 2022, aufrufbar unter <https://www.bloomberg.com/news/articles/2022-04-04/hacker-move-stolen-crypto-funds-from-ronin-breach-to-obfuscator> sowie die Medienmitteilung *Ronin Network*, Community Alert: Ronin Validators Compromised vom 29. März 2022, aufrufbar unter <https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r>.

248 Vgl. *de Miranda*, 2019, 10.01 ff.

249 *Weber/Yildiz*, 2022, 7; *Weber*, 2020, 280; *Weber/Studer*, 2016, 716 f. m.w.H.

Im weitesten Sinne umfasst die Cybersicherheit diejenigen Gefahren, die sich durch die Kopplung von gesellschaftlichen Vorgängen an die Digitalisierung ergeben. Die Cybersicherheit betrifft einerseits die Fähigkeit, Angriffen zu widerstehen, welche die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit digitaler Daten zu beeinträchtigen versuchen, d.h. die Sicherheit der Netzwerk- und Informationssysteme. Andererseits beschäftigt sie sich auch mit der Bekämpfung von Cyberangriffen sowie der Cyberverteidigung.[250]

Das Konzept der Cybersicherheit steht in engem Zusammenhang mit ähnlichen Konzepten, wie z.B. der «Informationssicherheit» oder «IT-Sicherheit» (bzw. «IKT-Sicherheit»). Die ISO/IEC-27000-Reihe definiert die Informationssicherheit als «*preservation of confidentiality, integrity, and availability of information*». Die Ähnlichkeiten zeigen sich in der Definition der Cybersicherheit als «*preservation of confidentiality, integrity, and availability of information in the Cyberspace*»; der Zusatz «Cyberspace» ist als «*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*» umschrieben.[251]

Zur Cybersicherheit gehört jedoch nicht bloss der Schutz von Informationen und Daten (also Datensicherheit), sondern auch der Schutz von nicht informationsbasierten Assets, die für IKT-Bedrohungen anfällig sind.[252] Die International Telecommunication Union (ITU) nimmt in ihrer Definition der Cybersicherheit den Schutz der Assets auf:[253]

«*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*»[254]

250 *Weber/Yildiz*, 2022, 7; *Calliess/Baumgarten*, 2020, 1150; ferner *Kosseff*, 2018, 988 f.

251 *Weber/Yildiz*, 2022, 8; die Definition der Cybersicherheit und des Cyberspace befindet sich in *ISO/IEC 27032:2012*, Information technology – Security techniques – Guidelines for cybersecurity, Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité.

252 Weber, 2020, 281.

253 *Weber/Yildiz*, 2022, 8.

254 Vgl. für die Definition der ITU, aufrufbar unter <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>.

Die «*organization and user's assets*» umfassen u.a. «*connected computing devices*». Gemäss ITU soll die Cybersicherheit gewährleisten, dass die Sicherheitseigenschaften der «*organization and user's assets*» gegen relevante Sicherheitsrisiken in der Cyberumgebung erreicht und aufrechterhalten werden. Zu den allgemeinen Sicherheitszielen gehören die Vertraulichkeit (engl. confidentiality), die Integrität (engl. integrity)[255] und die Verfügbarkeit (engl. availability); diese drei Aspekte werden oft als CIA-Triade bezeichnet.[256] Vertraulichkeit bedeutet, dass Informationen nicht unrechtmässig an unbefugte Personen, Prozesse oder Geräte weitergegeben werden. Zur Integrität gehört, dass die Informationen vor unbefugter Zerstörung oder Veränderung geschützt sind. Verfügbarkeit drückt aus, dass autorisierte Benutzer zeitnah und zuverlässig auf Daten und Informationen zugreifen können.[257]

Im Rahmen dieser allgemeinen Sicherheitsziele ist keine absolute Sicherheit zu erreichen; es gibt zahlreiche Möglichkeiten, Sicherheitslücken auszunutzen. Insbesondere die Verfügbarkeit der Systeme kann kaum zu 100% gewährleistet werden, da beim Einsatz von technischen Systemen jederzeit ein gewisses Ausfallrisiko besteht. Aus diesem Grund haben die Systeme nicht als *absolut sicher* zu gelten, sondern «bloss» den potenziell zu erwartenden Bedrohungen standzuhalten.[258]

b) Resilienz

Die Cybersicherheit allein genügt aber nicht, um ein stabiles und zuverlässiges System anzubieten; von Bedeutung sind auch die Widerstandsfähigkeit von Systemen und das Können, belastende Situationen zu meistern (sog. Cyber-Resilienz). Unter Resilienz ist die Fähigkeit von technischen Systemen zu verstehen, bei Störungen bzw. Teilausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrechtzuerhalten.[259] Theoretisch

255 Gemäss ITU kann die Integrität auch die die Authentizität und Unverfälschbarkeit umfassen.

256 *Weber*, 2020, 281. Diese allgemeinen Sicherheitsziele finden sich auch im ISG (*Meyer/Métille*, 2022, Rz. 15); im Detail zu den Sicherheitsmassnahmen im ISG, vgl. *Meyer/Métille*, 2022, Rz. 14 ff.

257 *Weber/Yildiz*, 2022, 8 f.; *Weber/Studer*, 2016, 717.

258 *Schultz/Sarre*, 2022, Rz. 10.

259 *Resilient*, 2020, 11.

betrachtet geht es um die Möglichkeit eines komplexen Systems, trotz massiver Störungen wieder in den Ausgangszustand zurückzukehren und grössere Systemzusammenbrüche zu vermeiden.[260]

Der Begriff der Resilienz findet sich – nicht zuletzt mit Blick auf eine interdisziplinäre Offenheit und Verknüpfung der Systeme – in neuerer Zeit auch in den Sozialwissenschaften, z.B. (i) als Fähigkeit von Gesellschaften, externe Störungen zu verkraften, ohne dass sich ihre wesentlichen Systemfunktionen ändern, bzw. (ii) als Beschreibung dynamischer Stabilitätseigenschaften ökologischer Systeme.[261] In ähnlicher Weise umschreibt der Bundesrat in Art. 3 lit. d CyRV die Resilienz als «die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen».[262]

c) Systemstabilität

Im Finanzmarktrecht spielt der Begriff der Systemstabilität eine besondere Rolle. Risiken für die Systemstabilität können von verschiedensten Faktoren herrühren, v.a. von Gefahren für die Cybersicherheit und die Cyber-Resilienz. Technologische Risiken betreffen insbesondere die Infrastrukturen. Mit Bezug auf Netzwerke, über die sich Zahlungen abwickeln lassen, sieht Art. 19 NBG ausdrücklich vor, dass die Nationalbank, um die Stabilität des Finanzsystems zu schützen, systemisch bedeutsame zentrale Gegenparteien, Zentralverwahrer und Zahlungssysteme (d.h. systemisch bedeutsame Finanzmarktinfrastrukturen) überwacht.[263]

Mit dem Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register sind die Anwendungsbereiche des NBG und des FinfraG zudem auf die Überwachung der DLT-Handelssysteme ausgeweitet worden. Die DLT-Handelssysteme können neben Handelsdienstleistungen für DLT-Effekten[264] (kryptobasierte Vermögenswerte) auch Nachhandelsdienstleistungen anbieten; folglich ist ein Angebot von Dienstleistungen im Bereich der Zentralverwahrung, Abrechnung oder Abwicklung möglich

260 *Weber/Yildiz*, 2022, 9; *Nagel*, 2020, 151 f.; vgl. ferner *Walker et al.*, 2006, 2.

261 *Walker et al.*, 2006, 2 f.

262 Vgl. auch *Weber/Yildiz*, 2022, 9.

263 Vgl. auch *Weber/Yildiz*, 2022, 10.

264 Vgl. im Detail Kap. III.A.1.a).

(Art. 73e Abs. 2 FinfraG).[265] Der Vorteil der DLT-Netzwerke besteht darin, dass die Abwicklung der Transaktionen in einem Peer-to-Peer Netzwerk ohne Intermediäre erfolgt und somit der Ausfall eines Teilnehmers ohne Probleme durch die restlichen Teilnehmenden kompensiert werden kann.[266]

Im Gegensatz zur Cyber-Resilienz bezieht sich die Systemstabilität auf die Fähigkeit, die Funktionen von Systemen auch in Anspannungsphasen oder Umbrüchen effizient abzuwickeln. Die Finanzsysteme müssen folglich in der Lage sein, Schocks zu absorbieren und dabei die essenziellen Funktionen des Systems zu gewährleisten. Insbesondere der Nationalbank obliegt die Aufgabe, die Solidität und Leistungsfähigkeit des schweizerischen Finanzsystems sicherzustellen.[267]

B. Sicherheit und Resilienz bei DLT-Handelsplattformen

Mit der dezentralen Speicherung der Daten auf DLT-basierten Netzwerken entfällt grundsätzlich der Single Point of Failure (dt. einzelner Ausfallpunkt), was die Nutzung eines – gestützt auf die Struktur – resilienteren Systems ermöglicht. Trotz dieser grundsätzlichen Resilienz auf DLT-Handelsplattformen gibt es – wie eingangs dargestellt – weiterhin verschiedene Angriffsmöglichkeiten, die insbesondere in Bezug auf Finanzmärkte Probleme bereiten können und den Regulator vor Herausforderungen stellt. Aus diesem Grund sind nachfolgend potenzielle Angriffsmöglichkeiten, insbesondere unter Abgrenzung zwischen herkömmlichen Angriffen und DLT-spezifischen Angriffen, darzustellen.

1. Herkömmliche Gefahren im Rahmen der DLT-Handelsplattformen

Als potenzielle, herkömmliche Gefahren in DLT-Systemen sind in erster Linie der Faktor «Mensch» (*a*)) sowie das Key Management (*b*)) zu erwähnen.

---

265 Vgl. Kap. III.C.1; vgl. ferner Komm. NBG-*Häusermann*, 2021, Art. 19 Rz. 5.

266 Vgl. hierzu *Drescher*, 2017, 206 f.; *Glatz*, 2018, 62; vgl. im Einzelnen dazu *Weber*, 2022, Rz. 39; vgl. auch Kap. II.A.1 und II.B.2.

267 *Nagel*, 2020, 149 f.; vgl. auch DBB, Glossar «Finanzstabilität», aufrufbar unter <https://www.bundesbank.de/action/de/723820/bbksearch?firstLetter=F>; OeNB, Finanzmarktstabilität, aufrufbar unter <https://www.oenb.at/finanzmarkt/finanzmarktstabilitaet.html>; EZB, Finanzstabilität und makroprudenzielle Politik, aufrufbar unter <https://www.ecb.europa.eu/ecb/tasks/stability/html/index.de.html>.

a) Faktor Mensch

Ähnlich wie in den «traditionellen» Finanzmärkten und bei den «traditionellen» Cybergefahren ist der Mensch auch in DLT-Systemen als erhebliches Risiko einzustufen; der Mensch gilt potenziell im Bereich der DLT als Weakest Link.[268] Der Mensch stellt ein grosses Risiko dar, weil er durch mutwillige oder unbedarfte Fehlmanipulationen die Sicherheit bzw. Resilienz der DLT-Systeme untergraben kann. Zudem gilt der Mensch als unüberblickbare Gefahrenquelle, da er mit seinen Handlungen auf jeder Ebene der herkömmlichen Gefahren mögliche Angriffsflächen zu eröffnen vermag. Deshalb lässt sich dieser Faktor nur mit regelmässigen Schulungen und Weiterbildungen bzw. mit regelmässigen Hinweisen auf die Gefahren steuern.[269]

b) Key Management

Auf DLT-basierten Systemen sind die Private Keys essenziell für den Zugang zur Authentifizierung von Aktivitäten bestimmter Handlungen.[270] Der Private Key birgt gleichzeitig aber ein Risiko, denn die Angreifenden sind mit dessen Besitz in der Lage, den Inhalt der Wallets zu entwenden. Aus diesem Grund ist jedes DLT-System dann unsicher, wenn die Private Keys nicht genügend gesichert sind.[271] Da der Verlust des Private Key zusätzlich eine Gefahr für das jeweilige DLT-System darstellen könnte,[272] besteht ein systembedingtes Interesse, die individuellen Fehler der Teilnehmenden zu reduzieren; die Anbieterinnen und Anbieter der Wallets offerieren deshalb verschiedene Key-Management-Dienste.

Ein stabiler Key-Management-Dienst ist von massgeblicher Bedeutung, da die meisten Cyberangriffe nicht die Blockchain selbst angreifen, sondern die Private Keys zu entwenden versuchen.[273] Beim Key Management ist insbesondere der menschliche Fehlerfaktor entscheidend und nicht die Sicherheit der

---

268 *Bissell/Lasalle/Dal Cin*, 2019, 9; *Camillo*, 2017, 199; *Webley/Hardy*, 2015, 353.

269 *Weber/Yildiz*, 2022, 26.

270 Vgl. zur Bedeutung der Private Keys und deren Sicherungsmöglichkeiten Kap. II.B.4.

271 *Pala/Alamb/Thakura/Singh*, 2021, 77; *Hon/Palfreyman/Tegart*, 2016, 14.

272 Es besteht die Gefahr, dass bei einem grossflächigen Angriff das Vertrauen in das DLT-System bzw. die Blockchain verloren geht. Ein Beispiel für einen grossflächigen Angriff über gestohlene Private Keys ist der Angriff auf das Ronin Network, vgl. Einleitung Kap. IV.A.1.

273 *English/Kim/Nonaka*, 2018, 12.

Blockchain an sich, da nicht die Blockchain unmittelbares Angriffsziel ist, sondern der Speicherort des Private Key;[274] oft handelt es sich dabei um Gefahren, die bereits im Rahmen der klassischen Cybersicherheit existieren.[275]

2. DLT-spezifische Herausforderungen

Die DLT-spezifischen Gefahren lassen sich grob in drei Unterkategorien aufteilen. Zunächst sind die konsens- und ledger-basierten Angriffe, also insb. der Finney-Angriff, der Wettlaufangriff (engl. race attack) und der 51%-Angriff, von Bedeutung (*a*)). Zudem sind auch die Angriffe auf das Peer-to-Peer Netzwerk selbst, also insb. der Sybil-Angriff und der Verdrängungsangriff (engl. eclipse attack), von Interesse (*b*)). Schliesslich gibt es auch Herausforderungen im Kontext der Smart Contracts (*c*)).

a) Konsens- und Ledger-basierte Angriffe

Das übergreifende Problem bei der DLT ist die Double Spending-Problematik; einfach ausgedrückt besteht beim Double Spending die Gefahr, dass derselbe Coin bzw. dieselbe Kryptowährung zweimal ausgegeben wird und die Angreifenden sich so einen monetären Vorteil sichern.[276] Das Double Spending ist grundsätzlich nur möglich, wenn nicht alle Nodes im Netzwerk denselben Informationsstand haben; es handelt sich also eigentlich um ein Problem der Synchronisation der Transaktion, da die Informationen einer Transaktion erst nach einer (in der Regel kurzen) Zeit an das Netzwerk übermittelt werden.[277] Das Double Spending lässt sich eigentlich nicht als eigene Kategorie von Angriff qualifizieren, sondern kann die Folge von verschiedenen Angriffen sein; dennoch ist offensichtlich, dass Double Spending insbesondere bei konsens- und ledger-basierten Angriffen vorkommt.[278]

---

274 Vgl. zur Sicherungsmöglichkeiten der Private Keys Kap. II.B.4.b).

275 *Eskandari/Barrera/Stobert/Clark*, 2018, 2 f.; zur Cybersicherheit in Finanzmärkten im Allgemeinen, vgl. *Weber/Yildiz*, 2022, insb. 21 ff. und 97 ff.

276 *Pérez-Solà/Delgado-Segura/Navarro-Arribas/Herrera-Joancomartí*, 2019, 451; vgl. zur Double Spending-Problematik auch Kap. II.A.2 mit Fn. 9.

277 *Sayeed/Marco-Gisbert*, 2019, 4 f. m.w.H.; *Rosenfeld*, 2014, 2.

278 Das Double Spending kommt insbesondere bei Wettlauf-, Finney- und 51%-Angriffen vor, jedoch kann auch bei einem Sybil-Angriff die Rede von Double Spending sein, vgl. *Iqbal/Matulevičius*, 2021, 76157; *Singh/Hosen/Yoon*, 2021, 13943.

Um das Risiko eines konsens- bzw. ledger-basierten Angriffs zu minimieren, hat das System dezentral zu bleiben, sodass nie eine Partei über alle Transaktionen im Netzwerk verfügen kann. In der Regel benutzen die DLT-Systeme spezielle Konsensmechanismen,[279] um dieser Gefahr entgegenzuwirken.[280]

aa) Finney-Angriff

Ein Finney-Angriff findet statt, wenn eine Transaktion bei null Bestätigungen durchgeführt wird (engl. 0-confirmation transaction). Beim Finney-Angriff haben die Angreifenden bereits einen Block geschürft (engl. mined), aber noch nicht an die übrigen Mitglieder des Netzwerks gesendet. In dieser Situation sind die Angreifenden in der Lage, eine Transaktion von der Adresse A1 an die externe Adresse A2 durchzuführen (die Transaktion T1). Denselben Token dieser T1 können sie an die Adresse B (ehrliches Mitglied des Netzwerks) senden und so die Transaktion T2 ausführen. Wie erwähnt, senden die Angreifenden die Transaktion T1 noch nicht an das Netzwerk, bevor die Transaktion T2 vom ehrlichen Mitglied akzeptiert wird. Da es sich bei der T1 um die frühere Transaktion handelt als bei T2 (und somit der Token von T2 bereits ausgegeben war zum Zeitpunkt der Transaktion T2), wird T2 rückgängig gemacht und das ehrliche Mitglied verliert den erhaltenen Token.[281]

bb) Wettlauf-Angriff (race attack)

Der Wettlauf-Angriff ist ebenfalls eine Art des Double Spending, er wird über die Kontrolle der Schürfgebühren (engl. fee of miners) vollzogen. Beim Wettlauf-Angriff senden die Angreifenden einen Token von der Adresse A1 an die Adresse B des ehrlichen Mitglieds des Netzwerks (Transaktion T1); daneben senden die Angreifenden dieselbe Anzahl Token an ihre eigene Adresse A2, jedoch mit einer höheren Transaktionsgebühr (Transaktion T2). Diese beiden Transaktionen finden auf zwei verschiedenen Blocks statt, sodass auf der Blockchain eine Fork (eine Gabelung bzw. ein neuer Strang) entsteht. Da die Transaktion T2 eine höhere Gebühr hat, ist die Wahrscheinlichkeit höher, dass die Transaktion T2 schneller in den Block auf dieser Fork geschürft wird; dadurch kann die Fork mit T2 schneller neue Blöcke anhängen. Dies führt dazu, dass der Block mit T2 früher bestätigt bzw. validiert wird als der Block mit T1; aus diesem Grund mutiert der Block mit T1 zu einem Waisenblock (engl.

279 Vgl. zu den Konsensmechanismen im Detail Kap. II.B.3.

280 *Aggarwal/Kumar*, 2021, 401 f.

281 *Wen/Lu/Liu/Huang*, 2021, 9; *Aggarwal/Kumar*, 2021, 402; *Vokerla et al.*, 2019, 5.

orphan block). Der Block besteht zwar weiterhin auf der Blockchain, aber ist nicht mehr Teil der Mainchain; folglich ist auch die Transaktion T1 rückgängig zu machen.[282]

cc) 51%-*Angriff*

Die Angreifer sind bei dieser Methode in der Lage, in einem neuen Strang neue Blöcke der Blockchain schneller zu produzieren als die übrigen Nodes im Netzwerk. Zu einem späteren Zeitpunkt wird dieser neue Strang dem Netzwerk mit dem Ziel präsentiert, den neuen Strang zu validieren. Dieser Prozess ist möglich, wenn die Angreifenden 51% der Rechenleistung der Miner (engl. hashing power) besitzen.[283] Der Grund liegt daran, dass z.B. beim Protokoll von Bitcoin festgelegt wird, dass der längste Strang der Blockchain zu befolgen ist; die Angreifenden können die übrigen Nodes im Netzwerk mit ihrer Rechenleistung überzeugen, den neu produzierten Strang zu berücksichtigen. Nach einer gewissen Zeit wird dieser längere, von den Angreifenden weitergeführte Strang Teil der Mainchain und der andere, ehrliche, aber langsamer weitergeführte Strang zum «orphan chain» (d.h. stehengelassen bzw. nicht mehr weitergeführt).[284] Dies führt zur Double Spending-Problematik,[285] d.h. zum Risiko, dass eine Kryptowährungseinheit zweimal ausgegeben wird.[286]

b) Angriffe auf das Peer-to-Peer Netzwerk

Neben den konsens- und ledger-basierten Angriffen sind auf DLT-Handelsplattformen auch Angriffe auf das Peer-to-Peer Netzwerk möglich. Mit dem Peer-to-Peer Netzwerk können die DLT-Systeme die verbesserte Sicherheit dieser Technologie umsetzen, indem die Nodes im Netzwerk das Protokoll

---

282 *Wen/Lu/Liu/Huang*, 2021, 9 f.; *Aggarwal/Kumar*, 2021, 402; *Iqbal/Matulevičius*, 2021, 76167; zum Orphan Block, vgl. *Lehar/Parlour*, 2021, 23 (insb. Fn. 22) und 27 ff. *Göbel/Keeler/Krzesinski/Taylor*, 2016, 26 ff. m.w.H.

283 Der Angriff ist auch möglich, wenn die Angreifenden weniger als 51% des Hashing Power besitzen, jedoch ist die Wahrscheinlichkeit eines erfolgreichen Angriffs bei sinkendem Besitz der Hashing Power kleiner; vgl. u.a. *Sayeed/Marco-Gisbert*, 2019, 5 und *Zhang/Lee*, 2019, 5715 m.w.H.

284 *Wen/Lu/Liu/Huang*, 2021, 10; Singh/Hosen/Yoon, 2021, 13943; *Aggarwal/Kumar*, 2021, 402 f.; *Akbar/Muneer/ElHakim/Fati*, 2021, 5 f.; *Li/Jiang/Chen/Luo/Wen*, 2020, 7 f.

285 *Aggarwal/Kumar*, 2021, 402; *Sayeed/Marco-Gisbert*, 2019, 4 f. m.w.H.; *Rauchs et al.*, 2018, 62; vgl. zur Double Spending-Problematik auch Kap. II.A.2.

286 *Pérez-Solà/Delgado-Segura/Navarro-Arribas/Herrera-Joancomartí*, 2019, 451 f.; vgl. ferner *Iqbal/Matulevičius*, 2021, 76157.

ausführen und eine identische Kopie der Transaktionen bzw. der Ledger besitzen. Obwohl das Peer-to-Peer Netzwerk gewisse Sicherheitsverbesserungen aufbringt, weist das Peer-to-Peer Netzwerk auch Gefahren auf, da spezifische Angriffe auf das Peer-to-Peer Netzwerk existieren.[287] Bei dieser Angriffskategorie nutzen die Angreifenden die Anonymität, den dezentralen Aufbau der DLT-Systeme sowie das Fehlen einer zentralen Autoritätspartei aus.[288]

aa) Sybil-Angriff

Ein Sybil-Angriff ist einfach ausgedrückt ein Angriff auf ein Peer-to-Peer Netzwerk durch Erstellung falscher Identitäten. Beim Sybil-Angriff ist zwischen den Honest Nodes, Sybil Nodes und Attacker Nodes zu unterscheiden.[289] Die Angreifenden kreieren bei diesem Angriff zahlreiche Sybil Nodes (grds. falsche Identitäten), die sie mit den Honest Nodes verbinden und so die «echten» Verbindungen zwischen verschiedenen Honest Nodes trennen. Im Ergebnis übernehmen die Angreifenden die Kontrolle über das Peer-to-Peer Netzwerk, sobald sie einen unverhältnismässig grossen Einfluss über das Netzwerk ausüben können. Sie vermögen so verschiedene Angriffe auf das Netzwerk auszuführen (u.a. Double Spending) und seiner Reputation zu schaden.[290]

Bei genauerer Betrachtung stationieren die Angreifenden eine bestimmte Anzahl Sybil Nodes im Netzwerk; jeder dieser Sybil Nodes ist mit je zwei Honest Nodes verbunden. Das Ziel der Sybil Nodes ist es, die Blockausbreitung auf dem DLT-System zu verzögern; hierfür stellen die Sybil Nodes eine grosse Anzahl gefälschter Identitäten her und sehen vor, dass diese Honest Nodes ihre Nachrichten bzw. Informationen an die Sybil Nodes senden. Dies führt dazu, dass nicht genügend Honest Nodes innerhalb der erforderlichen Zeit die Nachrichten und Informationen der anderen Honest Nodes erhalten.[291] Wichtig ist, dass die Zero Power Miners nicht in der Lage sind, neue Blöcke zu schürfen; ihre einzige Aufgabe ist, die Datenverbreitung zu steuern. Im Ergebnis leiten sie die Daten der Sybil Nodes weiter und halten so die Ausbreitung

287 *Aggarwal/Kumar*, 2021, 404.

288 Zum Sybil-Angriff auf Peer-to-Peer-Systeme, bereits *Douceur*, 2002, 251 ff.; zur Gefahr der Sybil-Attacke auf dem Bitcoinnetzwerk, *Bissias/Ozisik/Levine/Liberatore*, 2014, 149 ff.

289 Vgl. für die Bedeutung der Nodes in DLT-Systemen Kap. II.A.2, II.B.1 und II.B.3.

290 *Iqbal/Matulevičius*, 2021, 76156 f.; *Zhang/Lee*, 2019, 5715 ff., insb. 5716; vgl. ferner *Douceur*, 2002, 252 ff.

291 *Zhang/Lee*, 2019, 5716–5720; *Aggarwal/Kumar*, 2021, 404; *Rajab et al.*, 2020, 2; *Arifeen et al.*, 2021, 470 ff. *Kedziora/Kozlowski/Jozwiak*, 2020, 408 m.w.H.

der ehrlichen Blockchain an.[292] Mittels dieser Maximierung der Verzögerung der Blockausbreitung durch die Honest Nodes erhalten die Angreifenden die «Kontrolle» über das Netzwerk und können diese Situation ausnutzen, um z.B. einen Double Spending-Angriff durchzuführen.[293]

bb) Verdrängungsangriff (Eclipse Attack)

Im Gegensatz zum Sybil-Angriff, der das gesamte Netzwerk anvisiert, handelt es sich beim Verdrängungsangriff (engl. Eclipse Attack) um eine Vorgehensweise, bei der nur bestimmte Nodes angegriffen werden; beim Verdrängungsangriff haben die Angreifenden das Ziel, gewisse Nodes vom Netzwerk zu verdrängen. Dabei können die Angreifenden alle ein- und ausgehenden Verbindungen des Eclipsed Node kontrollieren und den Node vom Netzwerk isolieren. Beim Verdrängungsangriff, der ein Double Spending zum Ziel hat, erhalten nur der angegriffene Node bzw. die angegriffenen Nodes die Informationen zur Transaktion der Angreifenden, da der angegriffene Node von den Angreifenden vom Netzwerk isoliert wurde. Danach senden die Angreifenden an das gesamte Netzwerk eine zweite Transaktion mit denselben Token.[294]

c) Herausforderungen im Rahmen der Smart Contracts

Neben den erwähnten Problemen kommt im Rahmen der DLT-Handelsplattformen noch eine neuere, zusätzliche Gefahrenquelle hinzu, und zwar die potenziellen Herausforderungen hinsichtlich der Smart Contracts.[295]

Oft lassen sich die Angriffe auf Smart Contracts auf Programmierfehler zurückführen, wie dies auch beim eingangs erwähnten DAO-Hack der Fall war; der Smart Contract zielte darauf ab, Transaktionen vollständig zu automatisieren und jeglichen menschlichen Input zu beseitigen. Jedoch stellte sich im Nachhinein heraus, dass der Smart Contract verschiedenste Schwachstellen

---

292 *Swathi/Modi/Patel*, 2019, 2.

293 *Zhang/Lee*, 2019, 5716–5720; *Swathi/Modi/Patel*, 2019, 2.

294 *Wen/Lu/Liu/Huang*, 2021, 7 m.w.H.; *Iqbal/Matulevičius*, 2021, 76165 m.w.H.; *Singh/Hosen/Yoon*, 2021, 13944 m.w.H.; *Li/Jiang/Chen/Luo/Wen*, 2020, 16 m.w.H.; *Heilman/Kendler/Zohar/Goldberg*, 2015, 129 f.; *Singh/Ngan/Druschel/Wallach*, 2006, 1 f.

295 Vgl. zum Smart Contract Kap. II.B.5; für eine ausführliche Tabelle mit möglicher Taxonomie für Schwachstellen im Rahmen der Smart Contracts, vgl. *Singh/Hosen/Yoon*, 2021, 13946 m.w.H. und *Li/Jiang/Chen/Luo/Wen*, 2020, 12. Ebenfalls ausführlich *Perez/Livshits*, 2021, 1326 f. und *Jiang/Liu/Chan*, 2018, 260 f.

aufwies; z.B. sind die Angreifenden in der Lage, eine Anweisung zurück an sich selbst ausführen zu lassen und so die Kontrolle über Kryptowährungen zu erlangen.[296]

Denkbar ist zudem die Ausbeutung über die Zeitstempelabhängigkeit (engl. timestamp dependency). In der Blockchain hat jeder Block einen Zeitstempel; manchmal sind die Smart Contracts darauf programmiert, abhängig von einem bestimmten Zeitstempel eine Bedingung auszulösen. Da der Zeitstempel von der lokalen Zeit im System der Miner gesetzt wird, könnten wichtige Ausbeutungsmöglichkeiten entstehen, wenn diese in der Lage sind, den Zeitstempel zu modifizieren.[297]

Ähnlich verhält es sich bei der Blocknummernabhängigkeit: Die Smart Contracts können darauf programmiert sein, dass die Blocknummer Teil der Bedingungen für eine wichtige Operation (z.B. Transaktion von Kryptowährung) oder für die Generierung von zufälligen Nummern ist. Auch die Blocknummern sind der Gefahr ausgesetzt, von den Minern manipuliert und ausgenutzt zu werden.[298]

C. Regulatorische Herausforderungen und erforderliche Massnahmen für DLT-Handelsplattformen

1. Regulatorische Vorgaben für DLT-basierte Finanzmarktinfrastrukturen

a) Finanzmarktrechtliche Vorgaben

Der Gesetzgeber hat mit dem DLT-Gesetz sowohl neue Rahmenbedingungen für den (Sekundär-)Handel mit digitalen Aktiven als auch für die Errichtung von Handelsplattformen geschaffen; im Bereich der DLT-basierten Finanzmarktinfrastrukturen sind insbesondere Art. 73a ff. FinfraG von Bedeutung. Obwohl für die DLT-Handelssysteme spezifische Regelungen zur Sicherheit bzw. Resilienz fehlen, lassen sich verschiedene Vorkehren aus den gesetzlichen Vorgaben ableiten.

---

296 *Iqbal/Matulevičius*, 2021, 76171; *Li/Jiang/Chen/Luo/Wen*, 2020, 12; *Jiang/Liu/Chan*, 2018, 261. Diese Schwachstelle wird in der Literatur der Informatik auch Reentrency-Schwachstelle genannt.

297 *Li/Jiang/Chen/Luo/Wen*, 2020, 12; *Jiang/Liu/Chan*, 2018, 261.

298 *Jiang/Liu/Chan*, 2018, 261.

Zunächst hält der Gesetzgeber in Art. 73c Abs. 1 lit. c FinfraG fest, dass natürliche und juristische Personen an diesen Systemen zugelassen sind, sofern sie erklären, in eigenem Namen und auf eigene Rechnung teilzunehmen. Darüber hinaus hat das DLT-Handelssystem «ein Reglement über die Zulassung sowie die Pflichten und den Ausschluss von Teilnehmern [zu erlassen] und beachtet dabei insbesondere den Grundsatz der Gleichbehandlung» (Art. 73c Abs. 5 FinfraG); in diesem Reglement ist zu regeln, «ob und welche privaten Teilnehmerinnen und Teilnehmer [das System] zulässt» (Art. 58e Abs. 1 FinfraV). Aus den entsprechenden Vorgaben lässt sich ableiten, dass der Gesetzgeber – mindestens indirekt – die Errichtung der (öffentlichen) permissionless DLT-(Handels-)Systemen auszuschliessen beabsichtigt, da die Teilnehmenden auf diesen Systemen in der Regel anonym bleiben und keine Zugangsschranken haben. Als Konsequenz sind lediglich (private bzw. konsortiale) permissioned DLT-(Handels-)Systeme[299] erlaubt, weil der Zugang auf diese Systeme nur eingeschränkt möglich ist und die Teilnehmenden sich identifizieren müssen.

Ferner lässt sich aus der FINMA Berichtsvorlage zur «Mindestgliederung für den Prüfbericht betreffend das Bewilligungsgesuch für ein um Bewilligung ersuchendes Institut»[300] ableiten, dass grundsätzlich nur (private bzw. konsortiale) permissioned DLT-Handelssysteme zur Bewilligung zugelassen sind. In dieser Berichtsvorlage ist insbesondere das Kapitel «8.7 Geldwäschereivorschriften» relevant; seit dem Inkrafttreten des DLT-Gesetzes haben Handelssysteme für DLT-Effekten nach Artikel 73a FinfraG (also DLT-Handelssysteme) die Vorgaben des Geldwäschereigesetzes zu beachten (Art. 2 Abs. 2 lit. d^{quater} GwG). Gemäss Art. 3 Abs. 1 GwG müssen die Finanzintermediäre bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines beweiskräftigen Dokumentes identifizieren; gemäss Art. 4 Abs. 1 GwG ist weiter die wirtschaftlich berechtigte Person mit der nach den Umständen gebotenen Sorgfalt festzustellen. Diese GwG-Vorschriften schliessen die Möglichkeit aus, (öffentliche) permissionless DLT-Handelssysteme zu betreiben, da sowohl die Identität der Vertragsparteien den DLT-Handelssystemen bekannt sein muss als auch die jeweils wirtschaftlich berechtigte Person. Über die FINMA Berichtsvorlage erschliesst sich, dass die DLT-Handelssysteme nur bei Einhaltung dieser GwG-Vorschriften eine Bewilligung erhalten können, weshalb lediglich (private bzw. konsortiale) permissioned DLT-Handelssysteme realisierbar sind.

299 Vgl. für die Eigenschaften von permissionless und permissioned DLT-Systemen Kap. II.A.3.

300 FINMA, Mindestgliederung für den Prüfbericht betreffend das Bewilligungsgesuch für ein um Bewilligung ersuchendes Institut FINMA Berichtsvorlage, Bern 2021.

Ausserdem verlangt die «Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem nach Art. 73a ff. Finanzmarktinfrastrukturgesetz»[301] in «I.7 Handels- und Selbstregulierungsorganisation», dass u.a. ein Reglement über Zulassung, Ausschluss und Pflichten von Teilnehmenden (inkl. Teilnehmerkategorien) sowie Weisungen mit Ausführungsbestimmungen (z.B. betreffend technische Anbindung) erlassen werden. Dies deutet ebenfalls auf die Pflicht hin, bloss ein (privates bzw. konsortiales) permissioned DLT-System betreiben zu dürfen, da die Infrastrukturanbieter selbst die Zulassung der Teilnehmenden zu regeln und auch Ausschlussmöglichkeiten darzulegen haben.

Angesichts der Pflicht, nur (private bzw. konsortiale) permissioned DLT-(Handels-)Systeme zu betreiben, fallen verschiedenste (DLT-basierte) Sicherheitsgefahren dahin. Die bereits auf permissionless DLT-Systemen als theoretische Gefahr angesehenen 51%-Angriffe[302] sind auf permissioned DLT-Systemen grundsätzlich ausgeschlossen, da die Angreifenden aufgrund der Kontrolle des DLT-Handelssystems durch die Betreiber sich kaum in die Lage versetzen können, schneller neue Stränge auf der Blockchain zu generieren und zu validieren.

Da auf permissioned DLT-Systemen die Durchführung und Validierung einer Transaktion in der Regel auf die autorisierten Teilnehmenden beschränkt ist, sind auch der Finney- und Wettlauf-Angriff nicht denkbar. Der Finney-Angriff[303] als 0-Confirmation-Transaction müsste ausgeschlossen sein, da in einem solch kontrollierten Umfeld noch nicht bestätigte Transaktionen bei entsprechender Kontrolle der Teilnehmenden und Transaktionen nicht möglich sein dürften. Eine ähnliche Lage ist auch bei den Wettlauf-Angriffen[304] ersichtlich: Die frühere Bestätigung und Validierung einer Transaktion aufgrund der höheren Transaktionsgebühr dürfte ausgeschlossen sein, da die autorisierten Nodes auf permissioned DLT-Systeme nicht zwingend nach Transaktionsgebühr bestätigen und validieren, sondern andere Kriterien heranziehen können (und wohl heranziehen werden).

Auf ähnliche Weise sind die Sybil-Angriffe[305] auf permissioned DLT-Systemen praktisch ausgeschlossen, da sich die Angreifenden aufgrund der vorliegenden Aufsicht nicht mit Sybil Nodes bzw. falschen Identitäten an das Netzwerk an-

301 FINMA, Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem nach Art. 73a ff. Finanzmarktinfrastrukturgesetz vom 2. August 2021, Bern 2021.

302 Vgl. zur Vorgehensweise bei einem 51%-Angriff Kap. IV.B.2.a)cc).

303 Vgl. zur Vorgehensweise bei einem Finney-Angriff Kap. IV.B.2.a)aa).

304 Vgl. zur Vorgehensweise bei einem Wettlauf-Angriff Kap. IV.B.2.a)bb).

305 Vgl. zur Vorgehensweise bei einem Sybil-Angriff Kap. IV.B.2.b)aa).

schliessen können. Dasselbe Bild ergibt sich auch bei den Eclipse Attacks,[306] bei denen – im Gegensatz zu den Sybil-Angriffen – nicht das gesamte Netzwerk, sondern bloss einzelne Nodes Ziel des Angriffs sind. Diesbezüglich ist die erfolgreiche Ausführung des Angriffs ebenfalls praktisch ausgeschlossen, da ein permissioned DLT-System die falschen Identitäten bzw. die angreifenden Nodes vom Netzwerk ausschliessen können.

b) Datenschutzrechtliche Fragen

Im Rahmen des Datenschutzrechts ist insbesondere das «Recht auf Vergessen» bzw. die Möglichkeit, die Daten zu löschen, von Bedeutung. Das als Recht auf Vergessen umschriebene Konzept ergibt sich aus allgemeinen Grundsätzen (insbesondere aus der Zweckbindung und der Verhältnismässigkeit) sowie aus Art. 4 (insb. Abs. 2) aDSG, Art. 12 Abs. 2 lit. b aDSG und Art. 15 aDSG. Im am 1. September 2023 in Kraft tretenden, totalrevidierten nDSG ist zusätzlich zu den ähnlichen Vorgaben in Art. 4 nDSG, Art. 30 Abs. 2 lit. b nDSG, Art. 31 nDSG und Art. 32 nDSG auch die Löschung in der Definition des Begriffs «bearbeiten» enthalten (Art. 5 lit. d nDSG), ohne dadurch eine Legaldefinition für das Löschen zu schaffen.[307]

Auf DLT-basierten Finanzmarktinfrastrukturen stellt sich zudem die Frage, ob sie den relevanten datenschutzrechtlichen Vorgaben nachkommen können. Einerseits sind die Daten auf DLT-basierten Systemen aufgrund der transparenten Transaktionshistorie auf der Blockchain für die Teilnehmenden grundsätzlich einsehbar, andererseits erschwert die Unabänderlichkeit der Blockchain die Löschung gespeicherter Daten;[308] das Nachweisen der Löschung wird insbesondere dadurch erschwert, dass die Daten verteilt bei allen Nutzern gespeichert sind.[309]

Die transparente Transaktionshistorie könnte einer Verletzung der Datensicherheit nach Art. 5 lit. h nDSG gleichkommen, die als «Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder *Unbefugten offengelegt oder zugänglich gemacht werden*»,[310] definiert wird. Die Finanz-

306 Vgl. zur Vorgehensweise bei einem Eclipse Attack Kap. IV.B.2.b)bb).

307 Vgl. zum Ganzen *Rosenthal*, 2019, 190 ff.

308 Vgl. zur Möglichkeit der Löschung bzw. Änderbarkeit der Blockchain Kap. II.A.2, II.B.3.a) und II.C.3.a).

309 *Hon/Palfreyman/Tegart*, 2016, 15.

310 Hervorhebungen durch den Autor.

marktinfrastrukturen sind gemäss dem totalrevidierten nDSG gehalten, eine solche Verletzung der Datensicherheit zu melden, wenn sie «voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt» (Art. 24 Abs. 1 nDSG). Die DLT-Systeme können dieser Problematik aber zuvorkommen, indem sie auf permissioned DLT-Systemen die Einsicht in die Transaktionen nur den autorisierten Nodes bzw. Personen gewähren oder die Transaktionen genügend anonymisieren, sodass keine Personendaten offengelegt werden.

Die Problematik der Transparenz von Transaktionen auf der Blockchain[311] stellt sich selbst bei permissioned Systemen, da auch dort – gemäss dem grundlegenden Aufbau der DLT-Systeme[312] – die Transaktionen aufgrund der Transparenz für die Teilnehmenden einsehbar sind. Durch diesen Umstand besteht die Gefahr, dass die Daten Aussenstehenden bzw. den anderen Teilnehmenden bekannt gemacht werden; jedoch können die DLT-Systeme dieser Gefahr zuvorkommen, indem sie die Daten auf der Blockchain verschlüsselt, pseudonymisiert oder anonymisiert speichern (z.B. durch Implementierung einer Side-Chain).[313]

Eine Side-Chain ist eine sekundäre Blockchain, die mit der primären Blockchain verbunden ist. Die Side-Chains können eigene Konsensprotokolle besitzen, die sich vom Konsensprotokoll der primären Blockchain unterscheiden; sie werden u.a. zur Verbesserung des Datenschutzes, der Sicherheit der primären Blockchain und der Skalierbarkeit eingesetzt. Mittels Side-Chains lassen sich die Daten mit einer Hash-Referenz (engl. hash reference) an die Blockchain binden, während der Zugang zu diesen sensiblen Daten nur bestimmten, autorisierten Parteien erlaubt ist.[314]

c) Lösungsansätze mittels Soft Law und Sandboxen

Trotz der sicheren Technologie der DLT-basierten Systeme sind oft weitergehende Massnahmen für die Sicherheit erforderlich. Da Gesetze über ein formelles, oft langwieriges Verfahren zu erlassen sind, besteht das Problem,

311 Vgl. zur Transparenz der Transaktionen als Eigenschaft der DLT-Systeme Kap. II.B.3.a).

312 Vgl. zum Aufbau der DLT-Systeme Kap. II.A und II.B.

313 Vgl. zur Verschlüsselung bzw. Pseudonymisierung als Risikominderungsmöglichkeiten *Harasgama/Kleiner/Berger*, 2022, 44; *Bieri/Powell*, 2021, 782; für detailliertere Ausführungen zum gegenwärtigen Stand betr. pseudonymisierte Daten in der Schweiz, vgl. *Jotterand*, 2022, Rz. 49 ff., insb. Rz. 56.

314 Vgl. *Singha et al.*, 2020, 1 ff; *Nascimento/Pólvora*, 2019, 17 f.; *Maull et al.*, 2017, 483.

dass sich technologische Fortschritte und gesellschaftliche Veränderungen häufig nicht angemessen berücksichtigen lassen.[315] Aus diesem Grund nimmt Soft Law in sich technologisch schnell entwickelnden Sektoren mit steigender Tendenz eine «ersetzende» Rolle ein.

In solchen Konstellationen von nicht rechtzeitig vorhandenen, staatlichen Regulierungslösungen erlassen die involvierten Akteure materielle Bestimmungen, die nicht den Charakter eines formellen Gesetzes haben.[316] Gerade im Rahmen der Cybersicherheit und Cyber-Resilienz hat Soft Law eine grosse Bedeutung, da es Funktionen erfüllen kann, die früher mit formellen Gesetzen verbunden waren (z.B. Koordinierung der Akteure).[317] Die Selbstregulierung erlaubt die Implementierung von effizienten, flexiblen und auf reale Bedürfnisse reagierenden Regeln, die grundsätzlich auf Expertenwissen basieren und auf breite Akzeptanz stossen, da sie von den beteiligten Stakeholdern ausgehandelt werden.[318]

Soft Law in Form von Selbstregulierung vermag indessen nicht immer den ganzen Bereich eines gesellschaftlich erwünschten Rechtsrahmens abzudecken, weshalb es sinnvoll sein kann, wenn Soft Law von einem staatlichen Regime unterstützt wird. Dies ist der Fall, wenn der Staat grundlegende Regelungen nicht den privaten Akteuren allein überlässt, sondern in Form von «Co-Regulierungen» an der Gestaltung des regulatorischen Umfeldes mitwirkt.

Da die Risiken im Bereich der DLT-basierten Finanzmarktinfrastrukturen oft transnationaler Lösungen bedürfen, ist es angebracht, wenn die Länder ihre Gesetze und Richtlinien auf internationale Standards und Best Practices abstützen.[319] Obwohl für die Sicherheit und Resilienz der DLT-basierten Systeme noch keine internationalen Standards und Best Practices existieren, ist es sinnvoll, sich zumindest für die Grundzüge der internationalen Standards und Best Practices zur Cybersicherheit und Cyber-Resilienz auf «traditionelle» Informationstechnologien zu stützen.

Die «traditionellen» Ideen der existierenden Standards sind in ähnlicher Weise auf DLT-basierte Systeme übertragbar, d.h. bei der DLT braucht es ebenfalls Mechanismen zur Identifikation der Unternehmensrisiken, zum Schutz der

315 *Weber*, 2012, 10 ff.
316 *Weber*, 2014, 22 ff.
317 *Weber*, 2021b, 26.
318 *Weber*, 2014, 27.
319 *Weber*, 2021b, 28 f.

Systeme und zur frühzeitigen Erkennung der identifizierten Gefahren; ferner hat das DLT-basierte System angemessen zu reagieren und Wiederherstellungsmassnahmen einzuführen.[320]

Jedoch erfordert die Sicherheit und Resilienz in DLT-basierten Systemen ein konzeptionelles Umdenken, da diese Systeme nicht mehr zentral auf Unternehmensebene organisiert sind;[321] der Aufbau der DLT-Systeme führt dazu, dass kein Single Point of Failure[322] existiert. Aus diesem Grund erweist es sich als erforderlich, dass die Cybersicherheit auf der Ebene des gesamten Netzwerks gewährleistet ist. Angesichts dieser Verlagerung müssen sich die Organisatoren und Teilnehmenden ihrer Verpflichtungen bewusst werden, da in DLT-basierten Systemen jedermann zur Sicherheit beiträgt; dies ist auch in den zukünftigen Standards zu berücksichtigen.

In diesem Kontext ist auch an die Möglichkeit zur experimentellen Gesetzgebung zu denken. Eine solche Gesetzgebung dient dazu, den Regelungsgegenstand zu stabilisieren und neue, klare sowie abgrenzbare Massnahmen zu definieren. Experimentelle Gesetzgebung ist in der Regel angezeigt, wenn der Gesetzgeber (noch) nicht über genügend begründete Wirkungshypothesen verfügt und deshalb die Wirkungsweisen seiner zu treffenden Massnahmen (noch) nicht kennt.[323] Ausserdem ist die experimentelle Gesetzgebung bei komplexen Themen bzw. bei Themen, mit denen der Gesetzgeber wenig Erfahrung hat, geeignet;[324] zu diesen Bereichen gehören grundsätzlich auch Regulierungssegmente, die einem schnellen Wandel unterworfen sind, wie dies z.B. im Rahmen der DLT der Fall ist.

Da der Gesetzgeber nach der (überzeugenden) Konzeptphase die Experimentierphase in Form einer Verordnung, die zeitlich beschränkt ist, einleitet,[325] lässt sich die experimentelle Gesetzgebung eigentlich als Hard Law qualifizieren, aber behält gleichzeitig eine gewisse Nähe zum Soft Law; denn die als Hard Law zu qualifizierende Verordnung ist zeitlich begrenzt und lässt sich jederzeit ausser Kraft setzen, falls Probleme auftauchen sollten.[326] Im Kontext

320 Für die Cybersicherheit und Cyber-Resilienz, vgl. *Weber/Yildiz*, 2022, 21 ff.

321 Vgl. zum dezentralen Aufbau der DLT-Systeme Kap. II.A.2, II.B.1 und II.B.2.

322 Vgl. zum fehlenden Single Point of Failure aufgrund des Aufbaus der DLT-Systeme Kap. II.B.1.

323 *Mader/Rütsche*, 2004, 48 f.

324 *Chevallier*, 1996, 185; vgl. ferner *Montavon*, 2022, 809.

325 *Montavon*, 2022, 809.

326 Ein Gericht kann eine Norm der experimentellen Gesetzgebung für nicht anwendbar erklären.

der DLT vermag die experimentelle Gesetzgebung eine wichtige Rolle zu spielen, weil es dem Gesetzgeber möglich ist, sukzessive Nachbesserungen vorzunehmen; so können während dem Verfahren gleichzeitig neue Erkenntnisse aus der DLT vorliegen bzw. neue Infrastrukturen, Prozesse oder Formen in der DLT entstehen, die Teil der sukzessiven Nachbesserung werden.[327] Darüber hinaus weisen Normen, die aus experimenteller Gesetzgebung entstanden sind, auch ein höheres Sicherheitsniveau und eine höhere normative Dichte auf als Gesetze, die nicht gestützt auf Erfahrungswerte, sondern gestützt auf Annahmen ausgearbeitet wurden.[328]

Um die Wirksamkeit verschiedener (neuer) Regulierungen in Bezug auf innovative Modelle, wie z.B. die Sicherheit und die Resilienz in DLT-basierten Systemen, in einer sicheren Umgebung testen zu können, haben Behörden zudem die Möglichkeit der Sandboxen[329] geschaffen. Die Sandboxen haben verschiedene Ziele: Sie dienen zunächst der Erweiterung des Bewusstseins von Unternehmen bzgl. des bestehenden Rechtsrahmens; darüber hinaus fördern sie Innovation und erlauben den Behörden, die Risiken und Chancen im Bereich der Innovation besser abzuschätzen.[330]

Da es sich bei der Sandbox um einen geschützten Raum handelt, in welchem die Unternehmen ihre Vorhaben testen, erhalten sie Informationen, um sich selbst und weitere Marktteilnehmende bei einer späteren Anwendung der Erkenntnisse zu schützen und die Risiken zu minimieren.[331] Ausserdem ist es angebracht, während der (begrenzten) Testphase einzelne Vorschriften aufzuheben bzw. allenfalls neu vorgesehene Vorschriften einzuführen, damit eine angemessene Erprobung der DLT möglich ist;[332] jedoch sind auch hier Sicherheitsmassnahmen zu ergreifen, damit allfällige negative Folgen abgemildert werden können.[333] Schliesslich ist ein Austausch zwischen den betroffenen Unternehmen und den Behörden während der Laufzeit der Sandboxen erforderlich, damit diese rechtliche Interpretationshilfen für die normative Umset-

327 So auch *Montavon*, 2021, 431 ff.

328 *Montavon*, 2022, 810.

329 Financial Conduct Authority (FCA), Regulatory sandbox lessons learned report, 2017, 4, aufrufbar unter <https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf>.

330 ESMA/EBA/EIOPA Report, FinTech: Regulatory sandboxes and innovation hubs (JC 2018 74), aufrufbar unter <https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf>, 19 und 38.

331 *Volz*, 2022, 60.

332 Zu den Sandboxen im Rahmen der DLT vgl. *Zetzsche/Woxholth*, 2022, 212 ff.

333 *Volz*, 2022, 60; *Hagen*, 2020, 170.

zung der Ideen in der Sandbox abgeben können.[334] Als Beispiel von Sandboxen-Regulierungen sind sowohl die neue EU-DLT-Pilotregelung[335] als auch die FinTech-Bewilligung des Bundesrats der Schweiz zu nennen.[336]

2. Risikomanagement im Allgemeinen

Die regulatorischen Vorgaben können «nur» den groben Rahmen für eine grundlegende Sicherheit und Resilienz bieten. Die DLT-basierten Systeme haben innerhalb dieses Rahmens ihre Systeme sicher und resilient zu gestalten; dies geschieht in der Regel über das Risikomanagement der Unternehmen. Die DLT-Handelsplattformen sind in Bezug auf das Risikomanagement gehalten, «Methoden und Prozesse, die der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung und Berichterstattung von Risiken dienen», zu implementieren.[337] Innerhalb des Risikomanagements sind neben den herkömmlichen Risiken in Verbindung mit DLT-basierten Systemen insbesondere die DLT-spezifischen Risiken zu berücksichtigen, falls ein Unternehmen DLT-basierte Systeme betreibt.

Angesichts der neuen Technologien ist beim Risikomanagement ein stabiles Governance-Rahmenwerk für allfällige Massnahmen von grosser Bedeutung. Es obliegt den Leitungsorganen, einen übergeordneten Grundsatz für die Steuerung des Risikos festzulegen und dessen Beachtung sicherzustellen; dementsprechend sind sie verantwortlich für die Wahl der für ihre Tätigkeiten angemessenen Art des DLT-Systems. Ein gutes Rahmenwerk ist insbesondere mit Blick auf die kryptografischen Schlüssel und potenzielle Fehler im Smart

334 Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK), Regulatory Sandboxes – Best Practices für die Schweiz, Bericht vom 28. Februar 2020, 16 f.

335 Verordnung (EU) 2022/858 des Europäischen Parlaments und des Rates über eine Pilotregelung für auf Distributed-Ledger-Technologie basierende Marktinfrastrukturen und zur Änderung der Verordnungen (EU) Nr. 600/2014 und (EU) Nr. 909/2014 sowie der Richtlinie 2014/65/EU vom 30. Mai 2022, ABl. L 151, 1–33; vgl. für die ausdrückliche Benennung der Regelung als «Sandkasten» EDSB, 2021, 8.

336 In den Ausführungsbestimmungen zur FinTech-Bewilligung erwähnt das EFD und der Bundesrat, dass es sich bei Art. 6 BankV um einen bewilligungsfreien Bereich, also um eine Sandbox, handelt. Es wurde also im Rahmen der Sandbox für die Entgegennahme von bis zu CHF 1 Mio. ein bewilligungsfreier Raum geschaffen (vgl. EFD, 2018, 3, 8 f. und 11; *Bundesrat*, Bundesrat verabschiedet Ausführungsbestimmungen zur FinTech-Bewilligung vom 31.11.2018, aufrufbar unter <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-73186.html>).

337 FINMA, 2017b, Rz. 3.

Contract erforderlich, da die Angriffe zurzeit nicht zwingend auf die DLT-Systeme selbst, sondern auf die Gegebenheiten rund um die DLT-Systeme abzielen.

3. Risikomanagement im Rahmen der DLT-spezifischen Herausforderungen

Mit dem sich schnell entwickelnden Bereich der DLT haben auch die Cybersicherheitsmassnahmen Schritt zu halten, um die Risiken bei der DLT minimieren zu können. Die Architektur, der Einsatz und der Betrieb der permissioned DLT-Systeme haben Auswirkungen auf die dem Netzwerk inhärente Cybersicherheit und deren Gefahrenminimierung. Dabei sind die Anzahl und Art der Teilnehmenden auf der Blockchain, die Möglichkeit der Teilnahme von unbefugten Personen, die Gestaltung sowie Robustheit der Regeln für die Blockchain, der Konsensmechanismus, die Sicherheit der Verschlüsselungsprotokolle, die Abhängigkeit von externen Daten und die Fähigkeit, betrügerische, böswillige oder fehlerhafte Datensätze zu korrigieren, von entscheidender Bedeutung.[338]

Da diese Risikoquellen Bezugspunkte zur Cybersicherheit und Cyber-Resilienz bei «traditionellen» Systemen haben, sind mindestens als Hilfe die existierenden Gesetze, Richtlinien und die Selbstregulierungen der Industrie heranzuziehen. Folgende potenziell anwendbare Prinzipien fallen in Betracht:[339]

- Regeln für Zugangskontrollen zu den Kundeninformationssystemen, damit der Zugriff nur für autorisierte Personen erlaubt ist;
- Verfahren der doppelten Kontrolle und Aufgabentrennung;
- Verschlüsselung der Kundendaten (auch während der Übermittlung);
- Prüfungsprogramm zur Bewertung des Risikomanagements im Rahmen der Cybersicherheit, interne Kontrollsysteme sowie Vorkehren zur Einhaltung von Gesetzen, Vorschriften und internen Richtlinien in Bezug auf IT-bezogene Risiken;
- Gegen- und Wiederherstellungsmassnahmen, die bei unbefugtem Zugang zu Kundeninformationssystemen zu ergreifen sind.

338 Vgl. auch *English/Kim/Nonaka*, 2018, 17.

339 So auch *English/Kim/Nonaka*, 2018, 17; für Massnahmen im Rahmen des Risikomanagement und des Business-Continuity-Management auf Finanzmärkten im Allgemeinen vgl. *Weber/Yildiz*, 2022, 105 ff. m.w.H.

Da DLT-Systeme sich in einem schnell entwickelnden Umfeld entfalten, haben die Unternehmen mit Bezug auf das Risikomanagement breit abgestützt zu handeln und insbesondere auf allgemeine Empfehlungen zu achten. Aus diesem Grund ist für die DLT-Handelsplattformen ein ausgeprägtes Situationsbewusstsein (engl. situational awareness) von grundlegender Bedeutung. Das Situationsbewusstsein hat grossen Einfluss auf die Fähigkeit der Handelsplattformen, (DLT-basierten) Cybervorfällen zuvorzukommen oder schnell und effektiv auf sie zu reagieren. Hierfür ist insbesondere die aktive Teilnahme an Vereinbarungen über den Informationsaustausch und die Zusammenarbeit mit vertrauenswürdigen Akteuren innerhalb und ausserhalb der Branche unabdingbar.[340]

Die DLT-Handelsplattformen sind ausserdem gehalten, einen anpassungsfähigen Rahmen für die Cybersicherheit und Cyber-Resilienz auf DLT-basierten Systemen einzuführen, der sich mit der dynamischen Natur von Cyber-Risiken weiterentwickelt. Dies erlaubt den Handelsplattformen, mit den Entwicklungen in diesem sich schnell verändernden Bedrohungsumfeld Schritt zu halten, indem sie Sicherheitsbedrohungen und Schwachstellen identifizieren, bewerten und verwalten sowie geeignete Schutzmassnahmen frühzeitig in ihre Systeme implementieren.[341]

4. Risikomanagement im Rahmen der herkömmlichen Herausforderungen in Verbindung mit DLT-basierten Systemen

Da neben den DLT-spezifischen Herausforderungen weiterhin herkömmliche Gefahren (in Verbindung mit DLT-basierten Finanzmarktinfrastrukturen) von Bedeutung sind, haben die Finanzmarktinfrastrukturen auch die allgemeinen Vorgaben gemäss den jeweils anwendbaren Gesetzen, Richtlinien, Soft Law und Co-Regulierungen anzuwenden.

Von entscheidender Bedeutung sind Massnahmen zur Identifizierung der cybersicherheitsbezogenen Unternehmensfunktionen. Hierfür sind geeignete Prozesse und Kontrollen erforderlich, die gewährleisten, dass alle Risiken identifiziert, analysiert, gemessen, überwacht, gemeldet und innerhalb der

340 Für das Situationsbewusstsein auf Finanzmärkten bzgl. herkömmlichen Risiken vgl. *Weber/Yildiz*, 2022, 111 f. m.w.H.

341 Für den fortlaufenden Lernprozess und die Weiterentwicklung im Rahmen der Cybersicherheit und Cyber-Resilienz auf (herkömmlichen) Finanzmärkten vgl. *Weber/Yildiz*, 2022, 129 f. m.w.H.

Grenzen der Risikobereitschaft der Finanzmarktinfrastrukturen verwaltet werden. Die DLT-basierten Finanzmarktinfrastrukturen sind ebenfalls gehalten, kontinuierlich ihre Systeme zu überprüfen, damit sie einen angemessenen Cybersicherheits-Schutz bieten und Gegenmassnahmen planen können. Darüber hinaus sind mit geeigneten Sicherheitsinstrumenten, -strategien und -verfahren die Auswirkungen der Cyberrisiken zu minimieren.[342]

Insbesondere im Rahmen der Sicherung der Private Keys ist es denkbar, dass sich die Finanzmarktinfrastrukturen dazu entschliessen, einen eigenen Key-Management-Dienst anzubieten. Lokal (bei den Nutzern) gespeicherte private Schlüssel (engl. key in local storage) weisen aber einige Nachteile auf, da jedermann mit Zugriff auf den Ordner gestützt auf den Private Key die Schlüssel lesen kann. Zudem versuchen die Angreifenden oft mit herkömmlichen Methoden die Schlüssel zu stehlen; denkbare Konstellationen für einen Diebstahl sind die unfreiwillige Freigabe der entsprechenden Ordner (z.B. auf einem freigegebenen Netzlaufwerk) oder auch der physische Diebstahl eines Notebooks bzw. Smartphones.[343] Da bei der lokalen Speicherung insbesondere der menschliche Fehlerfaktor entscheidend ist[344] und nicht die Sicherheit der DLT an sich, erweist es sich als Vorteil, wenn die Finanzmarktinfrastrukturen einen individuellen Key-Management-Dienst anbieten können, welcher den eigenen Sicherheitsvorgaben in Bezug auf das Riskmanagement entspricht.

Ferner haben die DLT-basierten Systeme sachgerechte Mechanismen einzuführen, welche die potenziellen Cyberrisiken frühzeitig zu erkennen vermögen. Damit diese Mechanismen den internationalen Standards entsprechen und mit den Entwicklungen im Bereich der Cybersicherheit und der Cyberangriffe Schritt halten, ist es erforderlich, dass sie regelmässig getestet werden. Angemessen ist eine kontinuierliche Überwachung in Echtzeit oder nahezu in Echtzeit, welche die Finanzmarktinfrastrukturen beispielsweise mit der Einführung eines Security Operations Center erreichen können.[345] Diese Massnahmen vermögen insbesondere dabei zu helfen, Fehler im Code des Smart Contract frühzeitig zu erkennen und grösseren Schaden abzuwenden, da eine schnelle Reaktion möglich ist.

342 *Weber/Yildiz*, 2022, 107 f. m.w.H.

343 Für ausgewählte technische Massnahmen gegen herkömmliche Angriffsmethoden vgl. *Seiler/Griesinger*, 2022, Rz. 34 ff.

344 *Bissell/Lasalle/Dal Cin*, 2019, 9; *Camillo*, 2017, 199; *Webley/Hardy*, 2015, 353; so auch *Seiler/Griesinger*, 2022, Rz. 24.

345 *Weber/Yildiz*, 2022, 109 f. m.w.H.

Komplementär ist im Rahmen der frühzeitigen Erkennung von Cyberrisiken eine Plattform für den Informationsaustausch unter verschiedenen Finanzmarktinfrastrukturen ein effizientes Instrument. Mit dieser Plattform ist es weniger wahrscheinlich, dass gleiche oder ähnliche Cyberangriffe gegen verschiedene Unternehmen wirksam sind. Ziel der Plattform wäre, dass die anderen Finanzmarktinfrastrukturen mit der Meldung eines Cyberangriffs auf potenzielle Risiken vorbereitet sind und ihre Systeme anpassen können.[346]

346 *Weber/Yildiz*, 2022, 110 f. m.w.H.

V. Abwicklung von DLT-Handelstransaktionen

Neben einer funktionierenden Regulierung der DLT-Handelssysteme und der Erkennung potenzieller Sicherheitsrisiken in Verbindung mit der DLT bedarf es einer gefestigten rechtlichen Rahmenordnung für verschiedene Aspekte im Rahmen der Abwicklung von DLT-Handelstransaktionen. In diesem Kontext ist bezugnehmend auf die vorangehenden Kapitel die vertragliche Abwicklung von DLT-Handelstransaktionen zu untersuchen; dabei liegt der Fokus auf der Geschäftsabwicklung der zentralen und dezentralen Handelsplattformen sowie auf der Analyse gewisser Spezialfragen bei Transaktionsabwicklungen (A.). Danach werden die haftungsrechtlichen Herausforderungen bei DLT-Handelstransaktionen analysiert; in diesem Zusammenhang ist insbesondere zwischen der vertraglichen Haftung und der ausservertraglichen Haftung zu unterscheiden (B.).

A. Vertragliche Abwicklung von DLT-Handelstransaktionen

Die gesetzlichen Vorgaben zu den DLT-Handelsplattformen, die Eingang in das FinfraG gefunden haben (Art. 73a–Art. 73g), betreffen aufsichtsrechtliche Aspekte; geregelt werden etwa die Voraussetzungen zur Bewilligungserteilung, die von den Anbietern zu erfüllenden Handels- und Organisationspflichten, die Zulassung von Teilnehmenden und von DLT-Effekten sowie die zusätzlichen Pflichten bei weiteren Dienstleistungen.[347] Die neuen Gesetzesbestimmungen enthalten hingegen keine spezifischen vertragsrechtlichen Regeln. Für die rechtliche Beurteilung des Abschlusses und der Abwicklung von Handelstransaktionen ist deshalb auf die schon heute geltenden Vorgaben zurückzugreifen. Praktische Erfahrungen sind noch kaum vorhanden, weil die FinfraG-Normen zu den DLT-Handelssystemen erst am 1. August 2021 in Kraft getreten sind.[348]

---

347 Im Einzelnen dazu Kap. III.C und *Rolf H. Weber*, Handel mit digitalen Aktiven. In: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, Kap. VII Rz. 28 ff. (*Weber*, 2021a).

348 Der nachfolgende Text basiert in den Grundzügen auf *Rolf H. Weber*, Zivilrechtliche Aspekte von Geschäftsabwicklungen auf DLT-Handelsplattformen, SZW 2021, 450–460 (*Weber*, 2021c); dieser Beitrag wird nachfolgend nicht weiter referenziert.

Grundlage für die Abwicklung von DLT-Handelsgeschäften sind zivilrechtlich die Registerwertrechte. Das DLT-Gesetz hat insoweit eine neue rechtliche Ordnung geschaffen, und zwar durch die Einfügung von Art 973d–Art. 973i OR in das (traditionelle) Wertpapierrecht. Digitale Vermögenswerte (bzw. Token) können gestützt auf diese bereits seit dem 1. Februar 2021 in Kraft stehenden Bestimmungen als Registerwertrechte kreiert und mittels «Umbuchung» im Wertrechteregister übertragen werden.

Nachfolgend werden vorerst die Grundlagen der DLT-Handelstransaktionen (1.) und die verschiedenen Typen von DLT-Handelsplattformen erläutert (2.). Das Schwergewicht liegt hernach auf den vertragsrechtlichen Elementen der Transaktionsabwicklungen über DLT-Handelsplattformen (3.), die für die verschiedenen Handelsformen im Detail einschliesslich einzelner Sonderfragen zur Sprache kommen.

1. Wertpapierrechtliche Grundlagen der DLT-Handelstransaktionen

a) DLT-Effekten

Gemäss Art. 2 lit. a Ziff. 5b^{bis} FinfraG sind die DLT-Effekten[349] als Effekten in der Form (i) von Registerwertrechten (Art. 973d OR) oder (ii) von anderen Wertrechten, die in verteilten elektronischen Registern gehalten werden und die mittels technischer Verfahren den Gläubigern, nicht aber dem Schuldner, die Verfügungsmacht über das Wertrecht vermitteln, umschrieben. Nachfolgend im Vordergrund stehen die Registerwertrechte, die funktionell den verbrieften Wertpapieren entsprechen.[350]

DLT-Effekten sind immer auch Effekten und damit Finanzinstrumente (Art. 3 lit. a Ziff. 1 und lit. b FIDLEG). Technisch müssen sie in verteilten elektronischen Registern gehalten werden und die Verfügung erfolgt durch eine Umbuchung im Register; im Gegensatz zu traditionellen Effekten, deren Zirkulation der Mitwirkung eines Intermediärs bedürfen, lassen sie sich vom Inhaber direkt auf einen Dritten übertragen.[351]

349 Für detaillierte Ausführungen zu den DLT-Effekten, vgl. Kap. III.A.1.a).

350 Dazu nachfolgend Kap. V.A.1.b).

351 Vgl. Kap. III.A.1.a); *Eggen/Sillaber*, 2020, Rz. 5.

b) Wertrechteregister

Jedes Recht, das auch als Wertpapier ausgestaltbar ist (z.B. obligatorische Rechte, Mitgliedschaftsrechte [soweit vom Gesetz erlaubt] und einzelne Sachenrechte), lässt sich als Registerwertrecht ausgestalten;[352] die Vertretbarkeit des abgebildeten Rechts ist keine Voraussetzung.[353] Registerwertrechte erfüllen – wie traditionelle Wertpapiere und Bucheffekten – die Transport-, Legitimations- und Verkehrsschutzfunktion.[354]

Da das Wertrechteregister nur den Gläubigern und nur *im Grundsatz* mittels technischer Verfahren die Verfügungsmacht zu ermöglichen haben, sind die Betreiberinnen und Betreiber der Wertrechteregister insbesondere nicht gehalten, den Gläubigern *jederzeit* die Verfügung über die Registerwertrechte zu ermöglichen.[355]

Die (kaufgeschäftliche) Transaktionsabwicklung wird in Art. 973f Abs. 1 OR zwar nicht konkret umschrieben, sondern der Regelung in der Registrierungsvereinbarung überlassen. Aus der Anordnung, dass die Wirkungen namentlich am Eintrag im Register anknüpfen (Art. 973e OR), ergibt sich aber klar, dass auch der Vermögenstransfer durch «Austragung» des Verkäufers und «Eintragung» des Käufers im Wertrechteregister erfolgen muss (Art. 973f OR).[356] Der Gesetzgeber hat sich somit für eine funktionelle Parallelität zu den physischen Wertpapieren (Übergabe) und den Bucheffekten (Umbuchung) entschieden.[357]

Das Wertrechteregister erfüllt dementsprechend eine ähnliche Funktion wie etwa das Handelsregister oder das Grundbuch: (i) Der Anbieter des Wertrechteregisters ist verpflichtet (und einzig berechtigt), an den registermässig ausgewiesenen Gläubiger – unter Anpassung des Registers – zu leisten (Art. 973e

---

352 Für detaillierte Ausführungen zu den Wertrechteregistern und Registerwertrechten, vgl. Kap. III.A.1.b).

353 *Weber*, 2021e, Rz. 10.

354 Botschaft DLT-Gesetz, BBl 2020, 259; *Kuhn*, 2021a, Rz. 24 ff.; *Weber*, 2021e, Rz. 11; *Kramer/Meier*, 2020, 62; *von der Crone/Derungs*, 2019, 492.

355 Botschaft DLT-Gesetz, BBl 2020, 279; das vorübergehende Ausfallen des Wertrechteregisters (z.B. aufgrund von Wartungsarbeiten, Netzwerkstörungen oder Hackerangriffen) berührt die Wertpapierwirkung der Registerwertrechte nicht (vgl. auch *Kuhn*, 2021a, Rz. 58; *Kramer/Meier*, 2020, 63).

356 *Weber*, 2021e, Rz. 20; die Vorschriften zur Abtretung (Art. 164 ff. OR) kommen nicht mehr zur Anwendung.

357 Zur Sonderfrage, ob die Übertragung kausaler oder abstrakter Natur ist, vgl. hinten Kap. V.A.3.c)aa).

Abs. 1 OR). (ii) Die im Register gespeicherte Information gilt als richtig und der Gläubiger sowie Drittpersonen in gutem Glauben können sich – entsprechend wie im Recht der Orderpapiere (z.B. Namenaktien, Art. 1006 Abs. 2 OR) – darauf verlassen (Art. 973e Abs. 2 und 3 OR). Die lückenlose Aufzeichnung der Transaktionen im manipulationsresistenten, elektronischen Register ist somit vergleichbar mit der traditionellen Indossamentenkette, ohne dass ein Indossamentsnachweis vorzuliegen hätte.[358] Handelt der Erwerber nicht in bösem Glauben oder grobfahrlässig, bleibt der Rechtserwerb auch von einem Unberechtigten geschützt.

2. Typen von DLT-Handelsplattformen

a) Rechtsform von DLT-Handelsplattformen

Als neue Rechtsform schafft Art. 73a FinfraG das DLT-Handelssystem. Alternative DLT-Handelsplattformen sind aber denkbar und in der Praxis vorhanden, weshalb sich eine entsprechende Differenzierung aufdrängt.[359]

aa) DLT-Handelssysteme

Als DLT-Handelssystem[360] gilt gemäss Art. 73a Abs. 1 FinfraG eine gewerbsmässig betriebene Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie den Vertragsabschluss nach nicht-diskretionären Regeln bezweckt. Im Gegensatz zu den bestehenden multilateralen Handelsplätzen können die DLT-Handelssysteme neu auch natürliche Personen als Teilnehmende der Transaktionsabwicklungen zulassen.

DLT-Handelssysteme sind demgemäss eigenständig organisierte Handelsplätze für DLT-Effekten und weitere digitale Aktiven; handeln lassen sich deshalb auch andere tokenisierte Vermögenswerte (z.B. Zahlungs- und Nutzungs-Token).[361]

---

358 *Weber*, 2021e, Rz. 22; im Einzelnen dazu vgl. *Zellweger-Gutknecht/Monnerat*, 2021, 26 f.

359 Handelsplattform ist somit der umfassendere Begriff; von «Handelssystem» wird hier nur gesprochen, wenn die Voraussetzungen von Art. 73a FinfraG erfüllt sind. Zu den Wesensmerkmalen der DLT-Handelssysteme im Besonderen, vgl. Kap. III.C.1.b).

360 Vgl. für detaillierte Ausführungen zu den DLT-Handelssystemen Kap. III.C.

361 *Weber*, 2021a, Rz. 6, 9 und 38.

bb) Alternative DLT-Handelsplattformen

Alternative DLT-Handelssysteme «unterhalb» der vom FinfraG vorgegebenen Aufgreifkriterien erweisen sich als ein Bedürfnis, um kleinere Unternehmen nicht von vorneherein aus dem Markt für DLT-Handelsplattformen auszuschliessen. Die Rechtsunsicherheit ist insoweit aber im Moment noch recht gross. Die Swiss Blockchain Federation hat im Herbst 2020 (aktualisiert im Herbst 2021) einen Leitfaden für Unternehmen entwickelt, die sich für eine alternative Plattform interessieren.[362]

Als alternative Formen kommen, abgesehen von der Liquiditätsschaffung durch Market Makers, dezentrale DLT-Handelsplattformen mit beschränkten Funktionen, Bulletin Boards als Peer-to-Peer Netzwerke oder durch Emittenten organisierte Marktplätze in Frage.[363] Vertragsrechtlich gelten insoweit dieselben – nachfolgend zu vertiefenden – Überlegungen wie für DLT-Handelssysteme.

b) Ausgestaltung von DLT-Handelsplattformen

DLT-Handelsplattformen können grundsätzlich *dezentral* oder *zentral* organisiert sein.[364] Obwohl die DLT an sich eine dezentrale Infrastruktur darstellt, lässt sich das DLT-Handelssystem als (gleich zu umschreibende) zentrale «Einrichtung» ausgestalten; zudem liegt selbst bei dezentralen DLT-Handelssystemen keine vollkommene Dezentralität vor.[365] Ein vollkommen dezentrales Handelssystem ist denkbar als (i) one stop shop (ii) gestützt auf öffentlich ver-

362 SBF, 2021b, 9 ff.

363 Bei den alternativen DLT-Handelssystemen geht es vornehmlich um auftragsrechtliche Fragestellungen; für detaillierte Ausführungen zu diesen alternativen DLT-Handelsplattformen vgl. Kap. III.D.

364 Vgl. u.a. zur Differenzierung zwischen dezentralen und zentralen Handelssystemen auch Kap. III.D.2.b).

365 Vgl. auch *Eggen/Sillaber*, 2020, Rz. 19 f.; für detailliertere Ausführungen zur Dezentralität vgl. *Kramer/Meier*, 2020, 75 f. Gemäss der Swiss Blockchain Federation betreibt auch «Mt Pelerin» ein dezentrales Handelssystem, das gestützt auf einen besitzerlosen *Smart Contract* funktioniert und den Handel direkt zwischen den Teilnehmenden erlaubt; alle Teilnehmenden können auf diesen *Smart Contract* zugreifen und ihm Aufträge erteilen; der *Smart Contract* vermittelt Besitz über die Tokens dieser Aufträge und sammelt diese mit den Tokens aller anderen Aufträge; sobald eine Person ein entsprechendes Angebot abgibt und ein «Matching» vorliegt, wird die Transaktion abgeschlossen; da «Mt Pelerin» als Handelsplattform nicht in die Transaktion eingreifen kann, ist dieser *Smart Contract* ein gutes Beispiel für ein vollkommen dezentrales Handelssystem (vgl. SBF, 2021b, 16).

fügbare Software, die (iii) den Handel aus den eigenen Wallets der Teilnehmenden ermöglicht und (iv) die Private Keys nicht zentralisiert hält, sondern weiterhin bei den Teilnehmenden verbleiben lässt.[366] Im nachfolgenden vertragsrechtlichen Teil ist diese Differenzierung zwischen dezentralen und zentralen Plattformen zu konkretisieren.

Weiter ist davon auszugehen, dass nicht alle Schritte vom Vertragsabschluss (Matching) bis zur Abwicklung (Clearing, Settlement) zwingend auf der DLT-Handelsplattform ausgeführt werden müssen, sondern dass auch hybride Systeme eingerichtet werden dürfen (z.B. traditionelle Führung des Order Book und tatsächliche Abwicklung des Handels auf der DLT). Zwar fehlen entsprechende FinfraG-Bestimmungen, doch erscheint eine extensive Auslegung als sachgerecht.[367] In Anlehnung an die vom Bundesrat befürwortete Zulassung von Zahlungs- und Nutzungs-Token zum Handel auf DLT-Handelssystemen[368] lässt sich annehmen, dass die Abwicklung auch die Zahlungsseite mitumfassen kann, und zwar ungeachtet dessen, ob eine Kryptowährung oder Buchgeld geleistet wird. Da bei DLT-Handelssystemen regelmässig eine technische Untrennbarkeit von Handels- und Abwicklungsdienstleistungen vorliegt, ist konzeptionell davon auszugehen, dass die Anordnung von Art. 10 FinfraG zu den Nebendienstleistungen bei DLT-Handelssystemen eng auszulegen ist.

3. Geschäftsabwicklungen auf DLT-Handelsplattformen

Transaktionen mit digitalen Vermögenswerten basieren auf einer Vertragsbeziehung zwischen dem Verkäufer und dem Käufer des entsprechenden «Gutes». Die technische Ausgestaltung der DLT-Handelsplattform bleibt dabei nicht ohne Einfluss auf die vertragliche Qualifikation des Rechtsverhältnisses der Transaktionsparteien. Insbesondere ist die vorerwähnte Differenzierung in dezentrale oder zentrale DLT-Handelsplattformen genauer auszuleuchten. Nachfolgend wird deshalb zwischen den beiden Typen unterschieden; gesondert zu betrachten sind jeweils der Vertragsabschluss und hernach die Vertragsausführung.[369]

366 *Kramer/Meier*, 2020, 75 f. mit Fn. 156.

367 So schon *Weber*, 2021e, Rz. 40.

368 Botschaft DLT-Gesetz, BBl 2020, 311.

369 So schon *Eggen/Sillaber*, 2020, Rz. 18 ff.

Neben der transaktionalen Rechtsbeziehung zwischen Verkäufer und Käufer von digitalen Vermögenswerten besteht auch noch ein (hernach nicht weiter zu vertiefendes[370]) Vertragsverhältnis beider Parteien mit der Betreiberin der DLT-Handelsplattform, das die technisch fehlerfreie Abwicklung der Transaktion (d.h. des Verfügungsgeschäfts) über die angebotene Infrastruktur beinhaltet. Die rechtsgültige Übertragung von DLT-Effekten umfasst werkvertrags- und auftragsrechtliche Elemente; ein bloss zielgerichtetes Tätigwerden mit Blick auf das beabsichtigte Ergebnis (z.B. den Übergang der Verfügungsmacht) erscheint nicht als ausreichend, sondern der Erfolg der technisch veranlassten Token-Übertragung muss eintreten.

a) Dezentrale Handelsplattformen

Als dezentrale DLT-Handelsplattformen gelten diejenigen Infrastruktureinrichtungen, die zwar zentralisierte Teilleistungen erbringen (insbesondere die Führung des Orderbuchs), den Vertragsabschluss und die Vertragsausführung aber weitgehend ohne Miteinbezug ihrer Betreiberin ermöglichen.[371] Dezentrale DLT-Handelsplattformen räumen den Berechtigten einen direkten Zugang darauf ein; diese können somit auf die DLT-Effekten zugreifen und sie in der Folge auch selbstständig auf Dritte übertragen.[372]

aa) Vertragsabschluss

Bei den dezentralen DLT-Handelsplattformen erfolgen Handel und Transaktionsabwicklung gestützt auf einen Kaufvertrag (Art. 184 OR) direkt zwischen Verkäufern und Käufern. Die Betreiberin der DLT-Handelsplattform, die den Vertragsabschluss auf einem DLT-Handelssystem gemäss Art. 73a Abs. 1 FinfraG gestützt auf nicht-diskretionäre Regeln einzurichten hat, ist lediglich in der Rolle als Vermittlerin tätig, nicht auch als Partei der Werteübertragung; ihr fehlt die Verfügungsmacht über die Vermögenswerte der Teilnehmenden.[373] Die dezentralen DLT-Handelsplattformen haben immerhin teilweise die Möglichkeit, die Aufträge zu bestätigen, freizugeben oder zu sperren, um einen geordneten Handel sicherstellen zu können.[374]

---

370 Für weitere Ausführungen dazu vgl. hinten Kap. V.B.2.a)aa).

371 *Eggen/Sillaber*, 2020, Rz. 19.

372 *Eggen/Sillaber*, 2020, Rz. 22; *Kramer/Meier*, 2020, 75.

373 *Eggen/Sillaber*, 2020, Rz. 22.

374 *Bundesrat*, Bericht des Bundesrates vom 14. Dezember 2018 über rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf dem Finanzsektor, Bern, 14. Dezember 2018, 146 f. (*Bundesrat*, 2018).

Der transaktionsbezogene Vertrag kommt – wie erwähnt – zwischen dem Verkäufer und dem Käufer der DLT-Effekten zustande, und zwar automatisiert über die DLT-Handelsplattform. Durch die Zustimmung zur entsprechenden Transaktion unterwerfen sich die Vertragsparteien den technischen Vorgaben und den Regeln des Systems.[375] Zur Anwendung gelangen aus technischen Gründen nicht traditionelle (schriftliche oder mündliche) Vertragsformen, sondern der Vertrag muss unter Zuhilfenahme eines sog. Smart Contract abgeschlossen werden.[376]

Der Smart Contract stellt eine vertragliche Beziehung in digitaler Form mit Hilfe entsprechender Software dar, d.h. Leistung und Gegenleistung werden durch die gewählte Programmlogik vorgegeben. Die durch den Smart Contract ermöglichten Transaktionen von digitalen Vermögenswerten beruhen (vertragsähnlich) auf der in einem Code getroffenen «Abmachung», d.h. der definierte Leistungsaustausch ist auf der Basis des zur Durchführung vorbestimmten (determinierten) Codes abzuwickeln.[377] Eigenschaften von Smart Contracts sind die (unaufhaltbare) Selbstdurchsetzung, die (nicht anfechtbare) Unveränderbarkeit und die zeitliche Unbeschränktheit; die Vertragsabwicklung wird in Abhängigkeit von digital prüfbaren Ereignissen gesteuert, kontrolliert und dokumentiert.[378]

Weil die Bildung des gemeinsamen Willens zwischen den Kaufvertragsparteien auf der DLT-Handelsplattform ihren Niederschlag finden muss und insbesondere die Transaktionsabwicklung dort stattfindet, hat deren Betreiberin grundsätzlich den Smart Contract zur Verfügung zu halten und die erforderlichen technischen Kontroll- und Einflussmöglichkeiten bereitzustellen. Der Bundesrat will die Entwicklungen der Smart Contracts in diesem Zusammenhang abwarten und sieht eine spezifische Regulierung derzeit als verfrüht an.[379]

Vertragstypologisch ist die Beziehung zwischen den Vertragsparteien und der DLT-Handelsplattform als besondere Auftragsart zu werten; die DLT-Plattformbetreiberin ermöglicht technisch den Vertragsabschluss, d.h. sie vermittelt die Transaktionsabwicklung.[380] Im Vordergrund steht deshalb die Anwen-

375 *Eggen/Sillaber*, 2020, Rz. 23.

376 *Bundesrat*, 2018, 146.

377 Vgl. im Detail zum Smart Contract Kap. II.B.5; vgl. auch *Weber*, 2018a, 292.

378 *Weber*, 2018a, 292 m.w.V.; aus der Literatur vgl. weiter *Gyr*, 2019, 1 ff.; *Müller*, 2019, 330 ff.; *Müller/Seiler*, 2019, 317 ff.; *Eggen*, 2018, 155 ff.; *Furrer*, 2018, 103 ff.

379 *Bundesrat*, 2018, 86.

380 *Eggen/Sillaber*, 2020, Rz. 24.

dung der Regeln des Mäklervertrags (Art. 412 ff. OR), ergänzt durch die Bestimmungen des Auftrags (Art. 394 ff.). Von praktischer Bedeutung ist damit die Relevanz der Sorgfaltshaftung von Art. 398 OR; falls die Betreiberin der DLT-Plattform z.B. die technischen und organisatorischen Anforderungen an eine rechtssichere Geschäftsabwicklung nicht erfüllt, vermag ein Haftungsanspruch der Kaufvertragsparteien wegen mangelnder Auftragsabwicklung aufzuleben.

bb) Vertragsausführung

Mit Blick auf die Vertragsausführung (bzw. Vertragsabwicklung) ist zwischen der Effekten- und der Geldseite zu unterscheiden:

(i) Auf der *Effektenseite* wird die Transaktion nach dem Vertragsabschluss auf der DLT-Plattform ausgeführt, und zwar durch Übertagung der DLT-Effekten vom Verkäufer auf den Käufer.[381] Zivilrechtlich hat – wie erwähnt – eine Umbuchung im Wertrechteregister zu erfolgen.[382] Der Zeitpunkt und die Modalitäten des Übergangs beurteilen sich nach der Bestimmung von Art. 973f OR und der Registrierungsvereinbarung.[383] Die Lieferung lässt sich mit der Zahlung durch den Käufer verknüpfen, z.B. durch einen dezentral implementierten Treuhandmechanismus.

Das Gesetz legt nicht fest, ob der Konsensmechanismus[384] über eine zentrale Instanz (z.B. die DLT-Handelsplattform) oder dezentral über verschiedene Teilnehmende gesteuert wird. In einem echten dezentralen System müssen verschiedene, unabhängige Teilnehmende an der Validierung der Transaktion beteiligt sein, was die Abläufe je nach Konsensmechanismus verlangsamen könnte.[385] Bei sog. Forks[386] vermag dies zu Unsicherheiten über die Gültigkeit von Transaktionen zu führen; aus diesem Grunde dürfte sich in der Praxis künftig eher die Validierung der Transaktionen durch die DLT-Handelsplattform selbst durchsetzen.[387]

---

381 Vgl. vorne Kap. V.A.1.b).

382 Zu Inhalt und Form von Registrierungsvereinbarungen im Einzelnen vgl. SBF, 2021c, 11 (Ziff. 3) und *Eggen/Stengel*, 2020, 212.

383 *Eggen/Sillaber*, 2020, Rz. 25.

384 Zum Konsensmechanismus im Detail, vgl. Kap. II.B.3.

385 Dazu auch *Schurr*, 2019, 267; vgl. zum Konsensmechanismus im Detail, Kap. II.B.3.

386 Zum Begriff der Forks vgl. *Jacquemart/Meyer*, 2017, 471 ff; für weiterführende Bemerkungen zur Fork vgl. Kap. III.C.2.b)bb) mit Fn. 160.

387 *Eggen/Sillaber*, 2020, Rz. 25; vgl. auch *Europäische Kommission*, Impact Assessment, 2020, 64 m.w.H.

(ii) Um auf der *Geldseite* die Transaktion dezentral abwickeln zu können, müssen Zahlungs-Token auf der DLT-Plattform zur Verfügung stehen; diese Token sind ebenfalls als DLT-Effekten auszugestalten.[388] Die Abwicklung vermag damit direkt zwischen den Kaufvertragsparteien ohne Miteinbezug der Betreiberin der DLT-Handelsplattform zu erfolgen. Je nach Ausgestaltung dieser Zahlungs-Token (ggf. auch in der Form der weniger volatilen Stablecoins) besteht die Möglichkeit, beim Emittenten die «gewählte» Kryptowährung gegen eine Fiat-Währung umzutauschen.[389]

b) Zentrale Handelsplattformen

Als zentrale DLT-Handelsplattformen gelten diejenigen Infrastrukturen, bei denen die Kaufvertragsparteien deren Betreiberin als Intermediärin in die Transaktionsabwicklung miteinbeziehen müssen;[390] in dieser Konstellation sind also die Teilnehmenden auf die Mitwirkung der Betreiberin des Systems oder der nachgelagerten Infrastrukturträgerin angewiesen, weil sie keinen direkten Zugriff auf die Transaktionsabwicklung haben.[391] Sowohl die Zusammenführung von Angebot und Nachfrage als auch der Vollzug der Transaktionen erfolgt vielmehr durch die Betreiberin bzw. eine weitere Intermediärin.

aa) Vertragsabschluss

Auch bei zentralen DLT-Handelsplattformen ist vorausgesetzt, dass die Marktteilnehmer (d.h. die Kaufvertragsparteien) den Handel selbst mit Verkaufs- und Kauforders auslösen. Der Vertragsabschluss auf einer DLT-Handelsplattform wird regelmässig nach den von der Betreiberin der Infrastruktur festgelegten Regeln abgewickelt. Danach beurteilt sich auch, ob die Inhaber von DLT-Effekten über einen zugelassenen Intermediär (z.B. ein Wertpapierhaus) vorzugehen haben oder nicht.[392]

Erfolgt auf der Plattform ein direktes Matching von Angebot und Nachfrage, entsteht der Vertrag grundsätzlich zwischen dem Verkäufer und dem Käufer, d.h. es kommt ein Kaufvertrag (Art. 184 OR) zustande. Auf das Rechtsverhältnis zwischen der zentralen Handelsplattform als «Vermittlerin» und dem Verkäu-

388 Botschaft DLT-Gesetz, BBl 2020, 277.

389 Vgl. *Eggen/Sillaber*, 2020, Rz. 26 f.

390 *Eggen/Sillaber*, 2020, Rz. 20 und 28.

391 Die Verwahrung der Effekten erfolgt zentral (Art. 73a Abs. 1 lit. a FinfraG); *Eggen/Sillaber*, 2020, Rz. 28.

392 Vgl. *Eggen/Sillaber*, 2020, Rz. 29.

fer bzw. Käufer ist – wie bei dezentralen Handelsplattformen – der Maklervertrag (Art. 412 ff. OR), ergänzt durch Bestimmungen des Auftrags (Art. 394 ff. OR), anwendbar. Die technologisch ermöglichte, parallele Abwicklung von Effekten- und Geldseite eliminiert das Gegenparteirisiko des Geschäfts, weshalb sich in der Regel der Einsatz einer zentralen Gegenpartei erübrigt.[393]

Die Regeln der Betreiberin der Handelsplattform können – wie erwähnt – aber auch vorsehen, dass die Geschäftsabwicklung über eine zentrale Infrastrukturträgerin vorzunehmen ist. In diesem Fall tritt eine zugelassene Intermediärin in den Vertrag ein und es kommt zu einem doppelten, wenn zwar deckungsgleichen (Kauf-)Vertragsabschluss.[394] Wie im traditionellen Effektenhandelsgeschäft gelangt in dieser Konstellation vermutungsweise das Kommissionsrecht (Art. 425 ff. OR) zur Anwendung.[395] In diesem Kontext handelt die zugelassene Intermediärin als indirekte Stellvertreterin, die mit der Gegenpartei einen Kaufvertrag in eigenem Namen und auf fremde Rechnung, d.h. auf Rechnung des Kunden, abschliesst. Zwischen dem Verkäufer und dem Käufer entsteht deshalb kein direktes Vertragsverhältnis.[396] Angesichts der kommissionsrechtlichen Verweisung in Art. 425 Abs. 2 OR kommen die Sorgfalts- und Treuepflichten des Auftragsrechts zur Anwendung;[397] entsprechend haftet die Betreiberin der Handelsplattform für die Sorgfalt hinsichtlich ihres technischen Funktionierens und die zugelassene Intermediärin für die Sorgfalt hinsichtlich der korrekten Abwicklung der Verkaufstransaktionen.

Die Betreiberin der DLT-Handelsplattform darf nicht die Funktion einer zentralen Infrastrukturträgerin übernehmen, weil Art. 73a FinfraG die Funktionenkombination nur mit Bezug auf den Zentralverwahrer und die Zahlungsstelle erlaubt, nicht aber mit Bezug auf die zentrale Gegenpartei.[398]

---

393 In diesem Sinne das B2B-Geschäftsmodell der SDX (vgl. SIX Digital Exchange, aufrufbar unter <https://www.sdx.com/en/home/sdx/business-model.html>; dazu auch *Eggen/Sillaber*, 2020, Rz. 30.

394 *Weber* (Fn. 347), Kap. VII Rz. 133.

395 Vgl. BGE 133 III 221 E. 5.1 = Pra 96 (2007), Nr. 127; *Eggen*, 2011, 628; *Zobl/Kramer*, 2004, Rz. 1215. Zur Vermutung im Effektenhandel vgl. EBK, Bulletin 2008/51; EBK, Bulletin 47/2005, 157, Rz. 80.

396 *Eggen*, 2011, 628; vgl. auch *Zobl/Kramer*, 2004, Rz. 1215.

397 Vgl. BGer 4A_547/2012 vom 5. Februar 2013 E. 4.1.

398 Vgl. Kap. III.C.1.b) und III.C.1.c); so auch Botschaft DLT-Gesetz, BBl 2020, 311; *Eggen/Sillaber*, 2020, Rz. 30.

bb) Vertragsausführung

(i) Die *Effektenseite* der Transaktion wird entweder durch die Betreiberin der zentralen DLT-Handelsplattform oder über (eine) weitere Infrastrukturträgerin vorgenommen. Die Inhaber der DLT-Effekten haben keinen direkten Zugriff darauf, sie führen also nicht selber die Transaktion aus, sondern leiten die Übertragung nur ein; vielmehr veranlasst die Infrastrukturbetreiberin die Transaktionsausführung im Wertrechteregister.[399] Die Rechtsgrundlage für die Übertragung der Vermögenswerte liegt – wie erwähnt[400] – direkt in Art. 973f OR. Alternativ wäre dogmatisch ebenso eine analoge Anwendung des Anweisungsrechts (Art. 471 OR), das auch den traditionellen Buchgeldtransaktionen zugrunde liegt,[401] denkbar. Die Anweisung hat im neuen Umfeld der digitalen Werte indessen über das Wertrechteregister zu erfolgen, das die DLT-Effekten führt, um sicherzustellen, dass die Geldüberweisung parallel ausgeführt wird.[402]

Die Betreiberin der zentralen DLT-Handelsplattform legt auch den konkreten Konsensmechanismus fest. Gestützt darauf führt die DLT-Handelsplattform die Transaktion aus und bestätigt hernach diese zugleich. Aus diesen Gründen lässt sich sagen, dass zentrale DLT-Handelsplattformen grosse Ähnlichkeiten mit den konventionellen multilateralen Handelssystemen aufweisen. Der Vorteil von zentralen DLT-Handelsplattformen besteht darin, dass die Effektenseite stark mit der Geldseite verknüpft werden kann.[403]

(ii) Die *Geldseite* der Transaktionen lässt sich – entsprechend wie in der erwähnten Konstellation der dezentralen Plattform-Ausgestaltung – mittels Zahlungs-Token über die DLT-Handelsplattform abwickeln. Die Rechtsgrundlage liegt, da auch Zahlungs-Token sich als Registerwertrechte ausgestalten lassen,[404] in Art. 973f OR; alternativ kommt – wie zuvor erwähnt – die analoge Anwendung des Anweisungsrechts in Frage.

(iii) Genauer zu betrachten ist immerhin noch die Frage, ob die technologisch ermöglichte, parallele Abwicklung von Effekten- und Geldseite weiterhin als Abrechnung und Abwicklung zu gelten vermag. Entscheidend ist hierfür, ob Art. 73a Abs. 1 lit. c FinfraG mit dieser Simultanausführung das «zentrale Regis-

399 *Eggen/Sillaber*, 2020, Rz. 31.

400 Vgl. vorne Kap. V.A.1.b).

401 Vgl. dazu *Gauch/Schluep/Emmenegger*, 2020, Rz. 2313; *Eggen/Stengel*, 2020, 202.

402 *Eggen/Sillaber*, 2020, Rz. 33.

403 *Eggen/Sillaber*, 2020, Rz. 32.

404 Vgl. *Weber*, 2021e, Rz. 8; *Kuhn*, 2021a, Rz. 96; *Zellweger-Gutknecht/Monnerat*, 2021, 13 ff.

ter» umschreibt oder weitere Abrechnungs- und Abwicklungsdienstleistungen anvisiert. Gesetzessystematisch betrachtet verlangt Art. 73a Abs. 1 FinfraG, dass eine von drei Voraussetzungen für das Vorliegen eines DLT-Handelssystems (lit. a–c) erfüllt ist; Art. 73e Abs. 2 FinfraG statuiert «weitere Anforderungen». Würde Art. 73a Abs. 1 lit. c FinfraG bereits die Simultanausführung erfassen, wären die zusätzlichen Voraussetzungen von Art. 73e Abs. 2 FinfraG obsolet, weil dann alle DLT-Handelssysteme die Voraussetzungen zu erfüllen hätten. Aus diesem Grund dürfte die Simultanausführung nicht unter Art. 73a Abs. 1 lit. c FinfraG fallen.

Juristisch gesehen liesse sich auch mit der «logischen Sekunde» argumentieren, was zur Folge hätte, dass die Abwicklung der Effekten- und Geldseite auseinanderfallen und nicht mehr parallel ausgeführt würden. Eine solche Betrachtungsweise hätte aber zur Folge, dass gar keine Simultanausführung der Geschäfte mehr stattfinden könnte, was den eigentlichen Vorteil der zentralen Register untergraben würde.

c) Spezialfragen bei Transaktionsabwicklungen

aa) Kausalitäts- und Abstraktionsprinzip

Der Handel mit digitalen Vermögenswerten mittels Übertragung von Registerwertrechten beruht auf den Regeln des Kaufvertragsrechts und den Allgemeinen Bestimmungen des Obligationenrechts. Treten Störungen in der Vertragsausführung ein, sind die entsprechenden Rechtsbehelfe anwendbar. Für den Fall, dass die kaufvertragliche Wandelung oder eine Vertragsanfechtung (z.B. wegen mangelnder Geschäftsfähigkeit oder Grundlagenirrtum) geltend gemacht wird, stellt sich die Frage, wie die Rückabwicklung des bereits durchgeführten Geschäfts zur erfolgen hat. Insbesondere ist zu beurteilen, ob die Verfügung über digitale Vermögenswerte als kausaler oder abstrakter Rechtsvorgang zu qualifizieren ist.[405]

Das schweizerische Recht geht im Sachenrecht vom Kausalitätsprinzip aus; für Immobiliarsachen ergibt sich dies aus dem Gesetz (Art. 974 Abs. 2 ZGB), für Mobiliarsachen aus der ständigen Rechtsprechung des Bundesgerichts.[406] Bei der Abtretung (Zession) ist die Streitfrage trotz epischen Diskussionen

405 Zur Behandlung dieser Frage vgl. auch *Zellweger-Gutknecht/Monnerat*, 2021, 21 f.; *Weber*, 2021c, 458 f.; vgl. auch *Kramer/Oser/Meier*, 2019, Rz. 28.

406 Seit BGE 55 II 302 ff.; vgl. auch *Kuhn*, 2021a, Rz. 111.

seit Jahrzehnten nicht entschieden.[407] Das Bucheffektengesetz (BEG) hat sich nicht auf ein bestimmtes Prinzip festgelegt, sondern vielmehr versucht, die sich stellenden konkreten Fragen zu beantworten; tendenziell entspricht die Rechtslage eher dem Abstraktionsprinzip.[408]

Das DLT-Gesetz enthält keine Hinweise, ob für die Übertragung der Registerwertrechte das Kausalitäts- oder das Abstraktionsprinzip gelten soll. Der Bundesrat hat sich in der Botschaft für die kausale Betrachtungsweise ausgesprochen, unter Berufung auf die – als erwünscht erachtete – analoge Anwendung der traditionellen wertpapierrechtlichen Grundsätze sowie auf die überwiegenden Stellungnahmen in der Vernehmlassung.[409] Die Lehre hat sich in der Folge mehrheitlich, wenn zwar nicht einstimmig, für das Kausalitätsprinzip ausgesprochen.[410]

Das seit anfangs 2020 in Kraft stehende «Blockchain-Gesetz» im Fürstentum Liechtenstein bekennt sich demgegenüber zum Abstraktionsprinzip: Gemäss Art. 6 Abs. 2 TVTG[411] ist für eine wirksame Verfügung das Bestehen eines wirksamen Kausalgeschäfts nicht vorausgesetzt und eine etwaige Rückabwicklung eines nicht rechtswirksamen Geschäfts hat nach den Vorschriften des Bereicherungsrechts zu erfolgen.[412] Der Grund für diesen Entscheid liegt darin, dass die DLT-Systeme (z.B. Blockchain) grundsätzlich unveränderbar sind, weshalb das Kausalitätsprinzip zu einem Auseinanderklaffen zwischen der nominellen Rechtslage und den faktischen, auf dem DLT-System dokumentierten Verhältnissen führen würde.[413]

Die vorgenannte Diskrepanz ergibt sich aus den unterschiedlichen Blickrichtungen, welche für die Beurteilung der Schutzwürdigkeit relevant sein können: Das Kausalitätsprinzip entspricht (i) den Interessen des Verfügenden, z.B. zur Geltendmachung von Willensmängeln (nach erfolgter Verfügung über digitale Vermögenswerte), (ii) den Interessen von Dritten (z.B. Konkursgläubiger, der eine Aussonderung von Token im Konkurs beantragt) und (iii) den Interessen des wahren Berechtigten, der sein besseres Recht geltend machen will. Hin-

407 Vgl. *Meier-Hayoz/von der Crone*, 2018, § 2 Rz. 56 ff. m.w.V.

408 *Kuhn*, 2021a, Rz. 111; *Meier-Hayoz/von der Crone*, 2018, § 25 Rz. 1390 f.

409 Botschaft DLT-Gesetz, BBl 2020, 286.

410 *Weber*, 2021e, Rz. 21; *Kramer/Oser/Meier*, 2019, Rz. 28.

411 Gesetz über Token und VT-Dienstleister (VT = vertrauenswürdige Technologien) vom 3. Oktober 2019, LGBl. 2019 Nr. 301 (LR-Nr. 950.6).

412 Vgl. auch *Kuhn*, 2021a, Rz. 112.

413 Vgl. auch *Kuhn*, 2021a, Rz. 112; *Kuhn/Stengel/Meisser/Weber*, 2019, Rz. 43; a.M. wohl *Wyss*, 2019, Rz. 64 ff.

gegen kommt das Abstraktionsprinzip dem guten Glauben des erwerbenden Dritten und allgemein dem Geschäftsverkehr, der sich auf die Korrektheit des Wertrechteregisters (entsprechend dem Grundbuch und dem Handelsregister) abstützt, zugute.

Nicht relevant wäre die Frage der Anknüpfung für den Fall, dass Verpflichtungs- und Verfügungsgeschäft zusammenfallen würden. Diese Situation tritt in der Regel nicht ein, da auch bei auf Smart Contracts basierenden DLT-Handelsplattformen von einer zeitlichen Nachlagerung (zumindest im Sinne der «logischen Sekunde») auszugehen ist. Unter praktischen Gesichtspunkten lässt sich – im Sinne einer «Angleichung» der beiden Positionen – immerhin nicht übersehen, dass der Gutglaubensschutz – wie im Immobiliar- und im Mobiliarsachenrecht – das Kausalitätsprinzip zu überlagern vermag (Art. 933 ZGB); der gutgläubige Dritte ist also auch dann geschützt, wenn das Kausalitätsprinzip gilt.

In der Praxis dürften die Unterschiede zwischen den beiden dogmatischen Betrachtungsweisen nicht sehr gross sein bzw. kaum je relevant werden: Bei Anwendung des Kausalitätsprinzips wird in den meisten Fällen die Umlauffähigkeit eines digitalen Vermögenswerts über den Gutgläubigkeitsschutz gewährleistet sein. Für das Kausalitätsprinzip sprechen die Systemkohärenz mit Bezug auf alle Dispositionen von Vermögenswerten im ZGB und im OR sowie der stärkere (quasi-digitale) Rückübertragungsanspruch im Vergleich zum Bereicherungsanspruch (Art. 62 ff. OR). Die Folge, dass es im Wertrechteregister zu einer Zuordnungsanpassung (mangels technischer Möglichkeit des Löschens eines «Blocks» auf der Chain in der Form des «Überschreibens» des betroffenen Blocks zugunsten des Berechtigten) kommen muss, um das Auseinanderklaffen zwischen nomineller Rechtslage und faktischer Registerlage zu überbrücken, ist eine Aufgabe, die sich ohne allzu grossen Aufwand ausführen lässt.

bb) Finalität der Abwicklung

Die in Art. 973f Abs. 2 OR geregelte zivilrechtliche Finalität besagt, dass Verfügungen eines insolventen Gläubigers rechtlich verbindlich bleiben, wenn der Gläubiger sie vor der Konkurseröffnung in das System eingebracht hat (Ziff. 1), die Verfügungen nach den Regeln des Registers oder eines Handelssystems unwiderruflich geworden sind (Ziff. 2) und sie innerhalb eines Tages in das Register eingetragen wurden (Ziff. 3). Ob die Verfügungen unwiderruflich geworden sind, ergibt sich aus den Regeln des verwendeten Wertrechteregisters

oder aus der Verwendung eines anderen, übergeordneten Handels- oder Abwicklungssystems.[414] Ausserdem wird die tatsächliche Ausführung der Transaktion vorausgesetzt.

Im Falle der DLT-Handelsplattformen (z.B. Blockchain) gilt eine Transaktion als ausgeführt, sobald sie nach den Regeln der Register validiert ist. Dieser Prozess kann aber einige Zeit in Anspruch nehmen, was die Transaktion für eine unbestimmte Zeit in der Schwebe hält.[415] Um Manipulationsmöglichkeiten in dieser Schwebezeit einzuschränken, muss die Transaktion innerhalb von 24 Stunden nach Eingabe ausgeführt worden sein. Falls dies nicht geschieht, fällt der entsprechende Vermögenswert oder die Ersatzforderung in die Konkursmasse.[416]

Aufsichtsrechtlich ist die Finalität in Art. 89 FinfraG geregelt. Diese Bestimmung legt fest, dass Weisungen von insolventen Teilnehmenden an eine zentrale Abwicklungsinfrastruktur erst dann rechtlich verbindlich sind, wenn sie vor der Anordnung der Insolvenzmassnahme eingereicht wurden. Die Regelung von Art. 89 FinfraG, ergänzt durch Art. 73 FinfraV, legt die Einzelheiten auf der Effektenseite und auf der Geldseite fest. Auf dezentralen DLT-Handelssystemen wird keine Drittperson in die Abwicklung der Effektenseite einbezogen, weil die DLT-Effekten direkt vom Veräusserer auf den Erwerber übertragen werden.[417] In dieser Konstellation ist somit keine Anordnung i.S.v. Art. 89 FinfraG erforderlich. Liegt hingegen ein zentrales DLT-Handelssystem vor, könnte eine Anordnung erforderlich werden. Dieselben Überlegungen sind ebenso auf der Geldseite relevant.[418]

Im Zusammenhang mit DLT-Handelssystemen liesse sich aber auch argumentieren, dass die Anordnungen zur Finalität wegen der zeitlichen Verschränkung von Verpflichtungs- und Verfügungsgeschäft in Folge der Digital Ledger-Technologie überflüssig seien. Indessen bleibt zu beachten, dass sich die Abwicklung bei DLT-Effekten durchaus verzögern kann; die Unsicherheiten im Falle einer Insolvenz treffen aber bei einer dezentralen Organisation nicht die

414 Botschaft DLT-Gesetz, BBl 2020, 286 f.; vgl. auch Kap. III.C.5.a); *Eggen/Stengel*, 2020, 210 und 213; *Houdrouge/Tenot*, 2020, 61.

415 Botschaft DLT-Gesetz, BBl 2020, 287.

416 Vgl. auch Kap. III.C.5.a); vgl. auch Botschaft DLT-Gesetz, BBl 2020, 286 f.

417 Vgl. auch Kap. III.C.5.a).

418 *Eggen/Sillaber*, 2020, Rz. 42 f.

Infrastruktur, sondern die Teilnehmenden.[419] Ob der Systemschutz von Art. 89 Abs. 2 FinfraG auch mit Blick auf die Teilnehmenden zu greifen vermag, ist derzeit noch nicht geklärt.

Die Regelungen von Art. 973f OR und Art. 89 Abs. 2 lit. b FinfraG sind nicht identisch, weil aufsichtsrechtlich nur diejenigen Transaktionen, die an jenem Tag zur Ausführung kamen, «in dessen Verlauf die Massnahme angeordnet wurde», verbindlich und gegenüber Dritten wirksam sind.[420]

B. Haftungsrechtliche Konstellationen

Die Schaffung neuer (digitaler) Vermögenswerte und der geeigneten Infrastrukturen für Transaktionen verursacht in der Regel auch neue Haftungsrisiken. Die Bestimmungen des DLT-Gesetzes thematisieren die Haftung nur am Rande (Art. 973i OR: Informationshaftung), anders als der Vorentwurf des Bundesrates, der auch eine Haftung für die Einhaltung der Mindestanforderungen an ein Wertrechteregister vorsah.[421] Das bisher erschienene Schrifttum hat die Haftungsfragen für technisch verursachte Schäden weitgehend ausgeklammert.[422]

Im Mittelpunkt der Haftungsdiskussion stehen vornehmlich zwei Leistungsanbieter, nämlich die Betreiber von Wertrechteregistern und die Betreiber von DLT-Handelsplattformen.

419 Vgl. auch Kap. III.C.5.a).

420 *Ibid.*

421 Art. 973d Abs. 2 i.V.m. Art. 973h Abs. 2 VE-OR (dazu Eidg. Finanzdepartement, Erläuternder Bericht des Bundesrates zur Vernehmlassungsvorlage vom 22.3.2019, 36); verschiedene Stimmen in der Vernehmlassung haben dagegen eingewandt, dass der Schuldner damit für Risiken ausserhalb seines Einflussbereiches haften müsse, weshalb der Bundesrat auf diese Norm im E-DLT, das dem Parlament unterbreitet wurde, verzichtet hat.

422 Der nachfolgende Text basiert auf *Rolf H. Weber*, Haftungsfragen beim Handel von digitalen Vermögenswerten, SJZ 2021, 679–687 (*Weber*, 2021d); dieser Beitrag wird nachfolgend nicht referenziert.

1. Technische Abläufe und haftungsrechtliche Grundlagen

a) Differenzierung in verschiedene Layers

Was aus der Diskussion zu Haftungsfragen im Internet-Kontext bereits seit 25 Jahren bekannt ist, gilt für die Fruchtbarmachung der DLT im Rahmen von Handelsaktivitäten weiter: Eine Beurteilung nach dem Konzept «one size fits all» ist nicht möglich, d.h. Differenzierungen sind notwendig.[423] Insbesondere ist zwischen verschiedenen technischen «Layers» zu differenzieren: Im Internet-Kontext geht es z.B. um den Infrastruktur-, den Daten-, den Software- und den Applikationen-Layer sowie im DLT-Kontext von Decentralized Finance (DeFi) neu (in der US-amerikanischen Terminologie) um den Settlement-, Asset-, Protocol-, Application- und Aggregation Layer.[424] Im Rahmen des Handels mit digitalen Vermögenswerten liegt der Settlement Layer (z.B. Ethereum als DLT-Infrastruktur) auf der «untersten» Stufe. Weil die DLT definitionsgemäss ein dezentrales Protokoll darstellt, ist auch ihre Basis (d.h. der Settlement Layer) dezentral und damit nicht einer eindeutig bestimmbaren Einheit zurechenbar.

Der Settlement Layer setzt sich zusammen aus der DLT-Infrastruktur und den sog. Native Protocol Assets (z.B. die Kryptowährungen «BTC» oder «ETH» auf den jeweils entsprechenden DLT-Infrastrukturen) und ist – wie erwähnt – die Grundlage für weitere, darüber liegende Layers. Der Asset Layer besteht aus allen Vermögenswerten, die auf dem Settlement Layer herausgegeben werden; erfasst sind neben den genannten Native Protocol Assets insbesondere alle weiteren digitalen Vermögenswerte, die auf der betroffenen DLT-Infrastruktur herausgegeben werden (sog. Tokens).[425]

Für Handelstransaktionen sind vornehmlich der Protocol Layer sowie verschiedene Application Layers, die bestimmte Marktakteure einrichten, von Bedeutung. Der Protocol Layer bietet Standards für mannigfaltige Anwendungsfälle von z.B. dezentralen Handelsplattformen oder Derivaten an. Die Standards lassen sich grundsätzlich mittels Smart Contracts in die Blockchain implementieren und können von allen Nutzern (bzw. den von ihnen eingesetzten DeFi-Anwendungen) beansprucht werden. Der Application Layer vermittelt benutzerfreundliche Anwendungen, die mit dem jeweiligen Protocol

423 Vgl. dazu bereits vor 25 Jahren *Weber*, 1996, 531 ff.

424 Für die Internet-Layer vgl. schon früh *Weber*, 1996, 533 f. und für die DeFi-Layer neu *Schär*, 2021, 155 f.

425 *Schär*, 2021, 155 f.

Layer verbunden sind. Schliesslich erlaubt der Aggregation Layer als Erweiterung des Application Layer einen benutzerorientierten Zugang auf verschiedene Applikationen sowie Protokolle und bietet die relevanten Informationen in einer übersichtlichen Art und Weise an.[426] Die Betreiberinnen der einzelnen Layers lassen sich somit identifizieren, was die Zuordnung einer Haftung ermöglicht.

Sowohl die Zurverfügungstellung eines Wertrechteregisters als auch einer DLT-Handelsplattform beruht auf einer solchen Applikation, welche sich auf den Protocol Layer stützt. Denkbar und in der Praxis bereits vorhanden ist weiter das Angebot einer individuell entwickelten, umfassenden Dienstleistungspalette, z.B. neben dem Wertrechteregister parallel die Emission von Aktien oder die Verwahrung digitaler Vermögenswerte. Als möglich erscheint auch ein Modell, das sich dadurch auszeichnet, dass der Emittent die digitalen Vermögenswerte selber programmiert und veröffentlicht, womit «nur» der Protocol Layer benutzt wird, doch kann sich ggf. eine Haftung aus Fehlern bei der Programmierung ergeben.

Das DLT-Gesetz definiert das Wertrechteregister, das die Übertragung von Registerwertrechten ermöglicht, nicht konkret. In Berücksichtigung der teilweise kritischen Ergebnisse der Vernehmlassung zum Vorentwurf hat sich der Bundesrat entschieden, im Lichte der angestrebten Technologieneutralität «nur» die zentralen technischen Eigenschaften, die erfüllt sein müssen, um eine ausreichende Registerqualität zu erreichen, festzulegen (Art. 973d Abs. 2 OR).[427] Diese Anforderungen (Grundlage für rechtssichere Token-Übertragungen, Schutz der Integrität des Registers, Transparenzschaffung mit Bezug auf Rechte und Funktionsweise des Registers, Einsichtsrechte des Berechtigten) sind haftungsrechtlich relevant.

Das DLT-Handelssystem[428] wird in Art. 73a FinfraG umschrieben als «eine gewerbsmässig betriebene Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmenden sowie den Vertragsabschluss nach nichtdiskretionären Regeln bezweckt». Um bewilligungsfähig zu sein, sind weitere Voraussetzungen zu erfüllen. Abgesehen von den gesetzlich definierten DLT-Handelssystemen sind

426 *Schär*, 2021, 156.

427 Vgl. *Weber*, 2021e, Rz 14.

428 Für detaillierte Ausführungen zu DLT-Handelssystemen bzw. DLT-Handelsplattformen, vgl. Kap. III.C.1.

weitere DLT-Handelsplattformen denkbar und in der Praxis vorhanden, insbesondere von Anbietern, die ausserhalb des regulierten Bereichs ihre Dienstleistungen anzubieten bevorzugen.[429]

b) Anspruchsgrundlagen und Voraussetzungen

Mögliche Anspruchsgrundlagen eines durch einen Fehler betroffenen Berechtigten eines digitalen Vermögenswerts sind (i) die vertragliche Haftung, (ii) die ausservertragliche Haftung und (iii) die spezialgesetzliche Haftung. Mit dem Anbieter eines Wertrechteregisters oder einer DLT-Handelsplattform besteht in der Regel ein Vertrag, d.h. die vertraglichen Anspruchsgrundlagen, die den Geschädigten in eine gute Rechtsposition versetzen, sind damit verfügbar. Abgesehen von der praktisch nicht so bedeutsamen Deliktshaftung (Art. 41 OR) können auch spezialgesetzliche Haftungsnormen (z.B. DSG, PrHG, UWG) zur Anwendung kommen.

Um eine Haftung zu begründen, muss eine Pflichtverletzung oder ein widerrechtliches Handeln vorliegen, im DLT-Kontext insbesondere eine technische Fehlfunktion. Weiter vorausgesetzt sind der Eintritt eines Schadens sowie das Vorliegen des adäquaten Kausalzusammenhangs zwischen der Widerrechtlichkeit und dem Schadenseintritt. Schliesslich bedarf es eines Verschuldens, das im Vertrag vermutet wird und ausservertraglich nachzuweisen ist.[430]

Nachfolgend werden die zwei in der Praxis wichtigsten haftungsbegründeten Fallkonstellationen detaillierter erörtert, nämlich die Haftung für Programmier- und Technologiefehler sowie die Haftung für fehlerhafte Informationen.

Für die haftungsrechtlichen Anknüpfungspunkte sind auch die erläuterten Risikominimierungsmassnahmen von Bedeutung.[431] Das Risikomanagement gehört heute zu den zentralen Aufgaben der Compliance in jedem Unternehmen. Besonders im Kontext der Informationstechnologie hat sich das Konzept des Enterprise Risk Management (ERM) entwickelt; mit diesem Ansatz soll die verbesserte Implementierung angemessener technischer Schutzstandards und die intensivere Ausbildung des Personals realisiert werden.[432] Mit entsprechenden Schutzvorkehren lassen sich Haftungspotentiale einschränken und ist der Exkulpationsbeweis beim Verschulden leichter zu erbringen. Weiter von Bedeutung sein kann auch der Abschluss einer Versicherung, die nicht nur

429 Deshalb findet hier bewusst der Begriff der DLT-Handelsplattformen Verwendung.

430 Vgl. *Gauch/Schluep/Emmenegger*, 2020, Rz. 2486a m.w.V.

431 Vgl. auch Kap. IV.C.2.

432 Vgl. *Weber/Staiger*, 2017, 211.

etwaige Schäden zu decken vermag, sondern ggf. wirtschaftlich effizienter ist als die Auseinandersetzung nach einem Schadenseintritt wegen fehlerhaften Infrastrukturabläufen.[433]

2. Haftung für Programmiererinnen und Programmierer sowie Technologiefehler

a) Vertragliche Haftung

aa) Vertragsqualifikation

(1) *Anbieterin und Anbieter eines Wertrechteregisters*

Der Betreiber eines Wertrechteregister, dessen Qualitäten in Art. 973d Abs. 2 OR mit vier Kriterien umschrieben sind, verpflichtet sich gestützt auf die zwingend abzuschliessende Registrierungsvereinbarung gegenüber dem Token-Inhaber, im Falle des Verkaufs eines Token im Register dessen «Umbuchung» zugunsten des Erwerbers nach den Vorgaben des Gesetzes vorzunehmen. Diese Tätigkeit umfasst werkvertrags- und auftragsrechtliche Elemente. Da ein bloss zielgerichtetes Tätigwerden (Auftrag) das beabsichtigte Ergebnis, nämlich die rechtsgültige Übertragung eines Token, nicht zweifelsfrei zu erreichen vermag, ist davon auszugehen, dass die Registrierungsvereinbarung auch ein Erfolgselement beinhaltet, das werkvertraglich zu beurteilen ist.[434] Für den Betreiber einer DLT-Handelsplattform gelten kraft eines gesetzlichen Verweises die technischen Vorgaben des Wertrechteregisters in paralleler Weise.[435]

Gemäss Art. 973d Abs. 1 OR haben die Transaktionsparteien mit dem Betreiber des Wertrechteregisters eine Registrierungsvereinbarung abzuschliessen, die festhält, wie das Recht im Register eingetragen wird und dass dieses Recht nur über das Register geltend gemacht und übertragen werden kann. An die Stelle der Registrierungsvereinbarung vermag auch eine entsprechende statutarische Grundlage der z.B. tokenisierte Aktien ausgebenden Gesellschaft zu treten (Art. 622 Abs. 1 OR). Die Registrierungsvereinbarung muss zudem festlegen, nach welchen Regeln das Registerwertrecht übertragen wird, denn das

433 *Weber*, 2017b, 2017, 211 f.; vgl. dazu hinten Kap. V.B.2.a)cc).

434 Zur Abgrenzung zwischen Werkvertrag und Auftrag vgl. BSK OR-*Zindel/Schott*, Vor Art. 363-379 Rz. 4; BSK OR-*David Oser/Rolf H. Weber*, Art. 398 N 28.

435 Vgl. hinten Kap. V.B.3.a)bb).

Gesetz legt den Übertragungsmodus nicht selber fest, sondern verweist lediglich auf das zwingende Erfordernis einer solchen Vereinbarung (Art. 973d Abs. 1 und Art. 973f Abs. 1 OR).[436] Empfehlenswert sind weiter Regeln für den Fall, dass ein bestehendes Register in ein neues Register überführt wird (z.B. für Behebung von Fehlern oder einem technischen Upgrade).

Der Betreiber des Wertrechteregisters ist verpflichtet, dessen Funktionsweise durch angemessene technische und organisatorische Vorkehren sicherzustellen (Art. 973d Abs. 3 OR). Konkrete Vorgaben macht das Gesetz nicht und eine Verordnungs-Delegationsnorm fehlt. Der Betreiber ist aber für die Wahl des DLT-Systems (d.h. die technische Infrastruktur) zuständig und wird diese Wahl in der Praxis so ausüben, dass die Integrität und Funktionssicherheit des Registers gewährleistet ist.[437]

(2) *Anbieterin und Anbieter einer DLT-Handelsplattform*

Eine vergleichbare Beurteilung gilt für den Betreiber einer Infrastruktur, die als DLT-Handelsplattform dient; die Abwicklung des Handelsgeschäfts muss erfolgreich sein. Bei dezentralen DLT-Handelsplattformen erfolgen die Transaktionsabwicklungen zwischen den Vertragsparteien gestützt auf einen Kaufvertrag (Art. 184 OR); der Anbieter der Plattform ist lediglich als Vermittler tätig, da ihm die Verfügungsmacht über die Vermögenswerte fehlt. Im Vordergrund steht deshalb die Anwendung der Regeln des Mäklervertrags (Art. 412 ff. OR), ergänzt durch die Bestimmungen des Auftrags (Art. 394 ff. OR).[438] Auf zentralen DLT-Handelsplattformen können die Marktteilnehmer die Transaktionen ebenfalls selbst auslösen; in diesem Fall kommt bei einem «Matching» – wie bei dezentralen Handelsplattformen – ein Kaufvertrag zwischen dem Käufer und Verkäufer zustande. Sehen die Regeln der Handelsplattformbetreiberin jedoch vor, dass über einen zugelassenen Intermediär vorzugehen ist, tritt dieser grundsätzlich in den Vertrag ein, d.h. es kommt zu einem doppelten, wenn zwar deckungsgleichen (Kauf-)Vertragsabschluss; wie im traditionellen Effektenhandelsgeschäft gelangt in dieser Konstellation vermutungsweise das Kommissionsrecht (Art. 425 ff. OR) zur Anwendung.[439] Durch den kommissionsrechtlichen Verweis in Art. 425 Abs. 2 OR sind die Sorgfalts- und Treuepflichten des Auftragsrechts anwendbar.[440]

436 Vgl. auch SBF, 2021c, 11 f.

437 *Kuhn*, 2021a, Rz. 160.

438 Vgl. auch Kap. V.A.3.a)aa) und V.A.3.b)aa).

439 BGE 133 III 221 E. 5.1 m.w.V.; vgl. auch Kap. V.A.3.b)aa).

440 Vgl. BGer 4A_547/2012 vom 5.2.2013 E. 4.1.

Neben der Vertragsqualifikation mit Bezug auf die Abwicklung von Token-Transaktionen entsteht zwischen dem Verkäufer und dem Plattformanbieter sowie zwischen dem Käufer und dem Plattformanbieter auch noch ein Rechtsverhältnis, das die erfolgsgerichtete technologische Durchführung des Verfügungsgeschäfts beinhaltet. Entsprechend der Rechtsbeziehung mit dem Anbieter des Wertrechteregisters umfasst diese Tätigkeit werkvertrags- und auftragsrechtliche Elemente.[441]

bb) Rechtslage bei parallelen Anbieterinnen und Anbietern

Sind der Anbieter des Wertrechteregisters und der Anbieter einer DLT-Handelsplattform nicht identisch, stellt sich die zusätzliche Frage des Verhältnisses zwischen den beiden Marktakteuren, wenn bei der Abwicklung einer Transaktion eine Fehlentwicklung eintritt. Bestimmt der Token-Inhaber, auf welcher DLT-Handelsplattform eine Transaktion abgewickelt werden soll, bestehen parallele Ansprüche im Falle des Eintritts eines schädigenden Ereignisses; konkret ist also zu prüfen, welcher Marktakteur den (technischen) Fehler zu vertreten hat. Ermächtigt der Token-Inhaber den Betreiber des Wertrechteregisters, die DLT-Handelsplattform für die Verkaufstransaktion zu bestimmen, ist m.E. davon auszugehen, dass die Ausführung dieser Tätigkeit nicht zu einer Hilfspersonenhaftung (Art. 101 OR), sondern zu einer Haftung für den befugt eingesetzten Substituten (Art. 399 Abs. 2 OR) führt.[442] Bietet derselbe Marktakteur die Transaktionsabwicklung als Betreiber eines Wertrechteregisters und einer DLT-Handelsplattform an, trifft ihn bei Auftreten einer Fehlfunktion die nachfolgend zu erörternde Haftungsfolge.

cc) Werkvertragliche Erfolgshaftung

Die mangelhafte Abwicklung einer Transaktion mit digitalen Vermögenswerten stellt grundsätzlich eine vertragliche Pflichtverletzung dar. Wenn ein Technologiefehler (z.B. Datenkorruption, Funktionsunfähigkeit des Wertrechteregisters oder der DLT-Handelsplattform) zum Nichteintritt des beabsichtigten Erfolgs der Transaktionsausführung führt (Art. 363 OR),[443] spricht die

441 Vgl. vorne Kap. V.B.2.a)aa)(1).

442 Vgl. BSK OR-*Oser/Weber*, Art. 399 Rz. 2 f.

443 Zum Erfolgscharakter der Leistung des werkvertraglichen Unternehmers vgl. BSK OR-*Zindel/Schott*, Art. 363 Rz. 2. Die Haftungssituation zwischen der Herstellerin einer Plattform und deren Betreiberin, die werkvertrags-, kaufvertrags- und lizenzvertragsrechtliche Elemente aufweist, wird vorliegend nicht vertieft geprüft.

Lehre von einer technologisch mangelhaften Abwicklung, welche die Rechtsfolge der Sachgewährleistung auslöst (Art. 367 OR).[444]

Die Zurechnung an den Betreiber des Wertrechteregisters oder der DLT-Handelsplattform setzt indessen voraus, dass der Betroffene die entsprechenden Risiken auch tatsächlich zu beherrschen vermag. Mit Bezug auf solche Situationen hat die Lehre, nicht zuletzt im Kontext der Informationstechnologie, das Konzept der sog Risikosphärenhaftung entwickelt, das insbesondere in Deutschland im Werkvertragsrecht verbreitet zur Anwendung gebracht wird.[445] Jeder Vertragspartner ist verpflichtet, die in seiner Sphäre potenziell eintretenden Fehler zu verhindern oder zumindest zu minimieren. Die Haftung wird damit angeknüpft an die Möglichkeit, die Ausgestaltung der Transaktionsabläufe beeinflussen zu können; konkret geht es deshalb um die Frage, wie nahe die Risiken an den Handlungsmöglichkeiten des Anbieters einer Infrastruktur liegen.[446] Praktische Schwierigkeiten bei der Feststellung der erforderlichen «Nähe» lassen sich nicht übersehen; der Bereich der neutralen «Zone», die sich keiner Vertragspartei zuordnen lässt (z.B. unerwarteter Stromausfall, nicht vermeidbarer Hackerangriff, der die Infrastruktur blockiert), ist in der Realität relativ breit.

Die Zuordnung von Risikosphären lässt sich auf der Basis von Wahrscheinlichkeitshypothesen vornehmen. Tritt z.B. ein äusserlicher Faktor ein, mit dem ggf. zu rechnen gewesen ist, würde die Verantwortung diejenige Vertragspartei treffen, die mit einer solchen Wahrscheinlichkeit eher zu rechnen hatte. Vorausgesetzt wäre dabei nicht nur der Einsatz intelligenter Algorithmen, sondern die Vertragsparteien müssten die möglicherweise eintretenden Faktoren auch sachgerecht prognostizieren und in die codierte Transaktionsabwicklung integrieren können.[447]

Eine alternative Anknüpfungsmöglichkeit betrifft den Ansatz des «cheapest cost avoider»: Dieses Konzept sieht diejenige Vertragspartei als der Fehleranfälligkeit der Infrastruktur am nächsten stehend an, die in der Lage ist, den Schaden am effizientesten zu tragen.[448] Konkret kann es sich um die Person

444 Vgl. *Weber*, 2017c, Rz. 29; *Eggen* hat die Anwendung des Werkvertragsrechts auf SaaS-Verträge, die stark auf Computerprogrammen aufbauen, erneut analysiert und teilweise befürwortet (*Eggen*, 2021, 585).

445 BeckOK BGB-*Voit*, § 645 BGB Rz. 17 ff.; MüKo BGB-*Busche*, § 645 BGB Rz. 14 ff.; vgl. auch *Spindler*, 2007, Rz. 91.

446 BeckOK BGB-*Voit*, § 645 BGB N 21 ff.; MüKo BGB-*Busche*, § 645 BGB N 18.

447 *Weber*, 2017c, Rz. 32; *Marino/Juels*, 2016, 151 ff.

448 Für einen Überblick des Konzepts vgl. *Carbonara/Guerra/Parisi*, 2016, 173 ff.

handeln, die in angemessener Weise eine Versicherung abzuschliessen vermag. Zwingend ist ein solcher Ansatz aber nicht, weil es bei der Zuordnung der Verantwortung um die Relation zwischen der eingesetzten Technologie und der sie fachkundig entwickelnden Person geht.[449]

dd) Auftragsrechtliche Sorgfaltshaftung

Im traditionellen Vertragsrecht haben sich über die Jahrzehnte verschiedene Kriterien entwickelt, wie der anzuwendende Sorgfaltsmassstab zu bestimmen ist. Vom römisch-rechtlichen Standard des *pater familias* bis zur auftragsrechtlichen Sorgfaltspflicht (Art. 398 Abs. 2 OR) sind mannigfaltige Schattierungen möglich. Die Wahrnehmung der Sorgfalt im Sinne des auftragsrechtlichen Tätigkeitsgebotes beinhaltet die zweckgerechte, zweckmässige und «richtige» Verfolgung der Vertragsziele, und zwar gestützt auf eine objektivierte Betrachtungsweise.[450] Erforderlich ist somit, diejenige Sorgfalt anzuwenden, die ein gewissenhafter Vertragspartner (mit der vertraglich vorgesehenen Qualifikation) unter Berücksichtigung des spezifischen Vertragsinhalts und der besonderen Umstände des Einzelfalls bei der Besorgung des ihm übertragenen Geschäfts anwenden würde.[451]

Von Bedeutung ist, die in den konkreten Verhältnissen jeweils DLT-relevanten Parameter richtig vorauszusehen und sachgerecht in die Infrastruktur zu integrieren. Sowohl beim Angebot eines Wertrechteregisters als auch beim Angebot einer DLT-Handelsplattform stellt sich indessen das Problem, dass sich die neuesten technologischen Entwicklungen und die Auslegung des 2021 in Kraft getretenen DLT-Gesetzes in Einzelfragen nicht immer klar prognostizieren lassen, was dafür spricht, dass ein den gegebenen Umständen sowie den technischen und rechtlichen Unsicherheiten Rechnung tragender Standard an die Sorgfalt zu legen ist.[452]

449 *Weber*, 2017c, Rz. 31.

450 BSK OR-*Oser/Weber*, Art. 398 Rz. 24.

451 BGE 133 III 124; 115 II 64.

452 BSK OR I-*Oser/Weber*, Art. 398 Rz. 27; BK OR-*Fellmann*, Art. 398 Rz. 488; vgl. ferner Botschaft DLT-Gesetz, BBl 2020, 289.

b) Ausservertragliche Haftung

aa) Deliktshaftung

Die Deliktshaftung basiert auf dem allgemeinen Grundtatbestand der unerlaubten Handlung, d.h. eines deliktischen Verhaltens (Art. 41 OR);[453] alternativ wäre ggf. auch eine ausservertragliche Geschäftsherrenhaftung (Art. 55 OR) oder eine Werkeigentümerhaftung (Art. 58 OR) des Anbieters eines Wertrechteregisters oder einer DLT-Handelsplattform denkbar. In der Praxis stehen diese Konstellationen indessen im Kontext der Übertragung bzw. des Handels von digitalen Vermögenswerten nicht im Vordergrund, ausser etwa in Fällen des Hacking oder anderer widerrechtlicher Eingriffe Dritter in die Infrastruktur, weshalb eine vertiefte Analyse der konkreten Haftungsfragen unterbleibt.

bb) Spezialgesetzliche Haftung

Wie in vielen anderen Bereichen ebenso hat der Betreiber eines Wertrechteregisters oder einer DLT-Handelsplattform die Vorgaben des Datenschutzgesetzes einzuhalten. Regelmässig spielen bei der Übertragung bzw. dem Handel von digitalen Vermögenswerten auch Personendaten eine Rolle, die zu schützen sind. Das im September 2023 in Kraft tretende (neue) Datenschutzgesetz vom 25. September 2020 enthält nicht nur die Pflicht, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 8 nDSG), sondern will den Schutz von Personendaten auch durch Technik und datenschutzfreundliche Voreinstellungen sichern (Art. 7 nDSG); im Falle von erheblichen Risiken ist eine Datenschutz-Folgenabschätzung zu erstellen (Art. 22 nDSG). Fehlt es an den angemessenen Datensicherheitsvorkehren und haben unberechtigte Dritte deshalb Zugang zu Personendaten, lebt eine datenschutzrechtliche Haftung auf.[454]

Das Produkthaftpflichtgesetz ist auf körperliche Güter ausgerichtet; die notwendige Körperlichkeit ist nicht gegeben bei digitalen Vermögenswerten. Solange der Anwendungsbereich des Produkthaftpflichtgesetzes nicht erweitert wird, sind die Haftungsrisiken für die Anbieter insoweit gering. In der Europäischen Union ist zwischenzeitlich eine Anpassung des Anwendungsbereichs

453 Für einen Überblick vgl. *Weber*, 2017b, 210.

454 Im Einzelnen dazu *Rosenthal*, 2020, Rz. 43 ff. m.w.V.

geplant bzw. es gib immer wieder Vorstösse hierzu,[455] ohne dass bisher die Rechtslage eine Änderung erfahren hat; das Paket der Europäischen Kommission vom 28. September 2022 mit zwei Richtlinienvorschlägen zur zivilrechtlichen Haftung für Produkte und für Künstliche Intelligenz (KI) dürfte neuen Schwung in die Diskussion bringen;[456] immerhin hält der EuGH weiterhin an der Legaldefinition der «beweglichen Sache» fest.[457]

Geschäftsabwicklungen im Kontext des E-Commerce sind verbreitet spezialgesetzlich geregelt, verbunden mit besonderen Haftungsbestimmungen. Die Schweiz hat die EU-Richtlinie 2000/31 über den elektronischen Geschäftsverkehr[458] nicht umgesetzt, entsprechende Versuche sind gescheitert. Nur bezüglich der Impressumspflicht und einzelner Informationspflichten ist das UWG mit Parlamentsbeschluss vom 17. Juni 2011 durch spezifische Normen ergänzt worden (Art. 3 Abs. 1 lit. s und Abs. 2 UWG). Ziel dieser Gesetzesnovellierung ist gewesen, durch eine teilweise Angleichung des schweizerischen Rechts an die E-Commerce-Richtlinie das Vertrauen der Konsumenteninnen

455 Vgl. dazu schon *Weber*, 2017b, 210, und hernach Europäische Kommission, Konsultation: Zivilrechtliche Haftung – Anpassung der Haftungsregeln an das digitale Zeitalter und an die Entwicklungen im Bereich der künstlichen Intelligenz, aufrufbar unter <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Zivilrechtliche-Haftung-Anpassung-der-Haftungsregeln-an-das-digitale-Zeitalter-und-an-die-Entwicklungen-im-Bereich-der-k-nstlichen-Intelligenz/public-consultation_de>; Die Europäische Kommission hat ihrem Berichts über die Auswirkungen von KI, IoT und Robotik auf Sicherheit und Haftung bspw. einen Anpassungsbedarf der Produkthaftungsrichtlinie erwähnt, vgl. Europäische Kommission, Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung vom 19.02.2020, COM(2020) 64 final, aufrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020DC0064&from=DE>.

456 Vorschlag für eine Richtline «on liability for defective products», COM(2022) 495 final (aufrufbar unter <https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en>) und Vorschlag für eine Richtlinie «on adapting non-contractual civil liability rules to artificial intelligence», COM(2022) 496 final (aufrufbar unter <https://ec.europa.eu/info/files/proposal-directive-adapting-non-contractual-civil-liability-rules-artificial-intelligence_en>).

457 Urteil des EuGH vom 10. Juni 2021, *VI/KRONE – Verlag Gesellschaft mbH & Co. KG*, Rechtssache C-65/20, ECLI:EU:C:2021:471, Rz. 24 ff.; eingehend zum Entscheid auch *Seehafer/Hillebrand*, 2021, 1032 ff.

458 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt vom vom 17. Juli 2000, ABl. L 178, 1–16.

und Konsumenten in den Online-Handel zu stärken.[459] Die Anbieter von Wertrechteregistern und DLT-Handelsplattformen sind von den (allgemeinen) UWG-Normen in der Praxis indessen kaum betroffen, weil die nachfolgend zu erläuternden spezialgesetzlichen Informationsplichten[460] vorgehen.

3. Haftung für fehlerhafte Informationen

a) Informationspflichten

aa) Anbieterin und Anbieter eines Wertrechteregisters

Der Betreiber eines Wertrechteregisters ist verpflichtet, jedem Erwerber eines Registerwertrechts gewisse Informationen über dessen technische Ausgestaltung bekannt zu geben (Art. 973i Abs. 1 OR). Für Schäden, die dem Erbwerber durch unrichtige, irreführende oder den gesetzlichen Anforderungen nicht entsprechende Angaben entstehen, lebt eine Haftung des Betreibers auf (Art. 973i Abs. 2 OR). Diese Bestimmung ist der Haftung für die vollständige und korrekte Information bei einem zu veröffentlichenden Prospekt nachempfunden (Art. 69 FIDLEG).[461]

Gegenstand der Informationspflichten sind die Funktionsweise des Wertrechteregisters sowie die Massnahmen zum Schutz seiner Funktionsfähigkeit und Integrität. Zu informieren ist deshalb über die vier konstitutiven Merkmale eines Wertrechteregisters, nämlich die Verfügungsmacht, die Integrität, die Informationspflichten und die Verifizierungsrechte (Art. 973d Abs. 2 OR). Überdies ist offen zu legen, wie das Wertrechteregister organisiert ist und wie sichergestellt wird, dass die Funktionsfähigkeit gemäss Registrierungsvereinbarung gewährleistet wird. Teilweise gehören diese Informationen aber bereits zum Mindestinhalt, der im Wertrechteregister oder in mit ihm verknüpften Begleitdaten festzuhalten ist; fehlt es an diesen konstitutiven Elementen, liegt überhaupt kein Wertrechteregister vor und es kommt nicht zu einer rechtsgültigen Übertragung des Registerwertrechts, was die Informationspflicht nach Art. 973i OR überflüssig macht.[462] Eine ähnliche Überlegung gilt für die Informationen über den Inhalt des Wertrechts; dabei handelt es sich

459 Für einen detaillierten Überblick zur UWG-Revision vgl. *Weber/Wolf*, 2012, Rz. 6 ff.

460 Vgl. dazu nachfolgend Kap. V.B.3.

461 Vgl. Vernehmlassungsvorlage (Bundesgesetz Vorentwurf zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register), 9; *Kuhn*, 2021a, Rz 162.

462 *Kuhn*, 2021a, Rz. 165.

um Informationen, die notwendig sind, um ein bestimmtes Registerwertrecht eindeutig bestimmen zu können (Art, Nominalwert, Stückelung des betroffenen Rechts).[463] Eine Erweiterung des Informationsumfangs würde sich wertpapierrechtlich indessen nicht rechtfertigen lassen.

Nach Art. 973i OR beschränken sich die Informationsanforderungen auf technische Aspekte und gehen damit deutlich weniger weit als vergleichbare ausländische Rechtsgrundlagen. So sehen z.B. die voraussichtlich im Jahre 2023 in Kraft tretende europäische Verordnung zu den Kryptowerten (Art. 14 MiCA)[464] und das liechtensteinische Recht (Art. 30 ff. TVTG) eine Haftung für Informationen im Kontext einer Emission digitaler Vermögenswerte vor. Diese prospektähnliche Haftung soll gewährleisten, dass der Emittent eines Kryptowerts nicht unvollständige, unfaire oder nicht eindeutige Informationen zur Verfügung stellt, die zu einem Schaden führen. Da Art. 973i OR auf technische Aspekte beschränkt ist, fehlt damit den Anlegern in der Schweiz eine Haftungsgrundlage, sofern keine Prospektpflicht besteht bzw. sofern einer der in der Praxis nicht selten greifenden Ausnahmefälle der Prospektpflicht greift.[465]

Gesamthaft lässt sich indessen nicht übersehen, dass die Informationspflichten zu den technischen Aspekten recht unbestimmt formuliert sind; dies ist nicht unproblematisch, soweit es sich um technische Fragestellungen handelt, die für den Informationsadressaten nur als sinnvoll erscheinen, wenn er sie verstehen und verarbeiten kann (Problem des mangelnden Vorwissens). Verständlichkeit des Informationsinhalts und Umfang der Informationen müssen somit einen sinnvollen Ausgleich erfahren, der sich ggf. durch von Branchenverbänden noch zu erarbeitenden Standards erreichen lässt.[466]

---

463 *Kuhn*, 2021a, Rz. 167.

464 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937, COM/2020/593 final. Der Trilog zwischen den gesetzgebenden Organen ist bereits abgeschlossen; der Europäische Rat und das Europäische Parlament müssen die MiCA nur noch formal annehmen (vgl. Rat der EU, Digitalisierung des Finanzwesens: Einigung über die europäische Verordnung über Kryptowerte (MiCA) – Pressemitteilung vom 30.06.2022, aufrufbar unter <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>.

465 *Kuhn*, schreibt dazu: «Diese Lösung ist nicht wirklich befriedigend und sollte de lege ferenda überprüft werden.» (*Kuhn*, 2021a, Rz. 164).

466 Vgl. auch *Kuhn*, 2021a, Rz. 167.

Adressat der Informationspflichten ist jeder Erwerber, d.h. zunächst der erste Nehmer des digitalen Vermögenswertes, der mit dem Emittenten einen Begebungsvertrag abschliesst und ein Registerwertrecht erwirbt. Nach der bundesgerichtlichen Praxis zur Prospekthaftung, die vorliegend analog anzuwenden ist, kann sich aber auch jeder spätere Erwerber auf die Informationspflichten berufen.[467]

bb) Anbieterin und Anbieter einer DLT-Handelsplattform

Für die Betreiber einer DLT-Handelsplattform sieht das DLT-Gesetz keine Haftungsnorm vor, die parallel zu Art. 973i OR spezifische Informationspflichten verankert. Sind die Voraussetzungen einer Prospektpflicht nach Art. 35–37 FIDLEG erfüllt, ist deren Beachtung auch beim Handel mit digitalen Vermögenswerten auf einer DLT-Plattform erforderlich (Art. 73d Abs. 1 Satz 2 FinfraG). Im Übrigen sind die für andere Handelsplätze geltenden Anforderungen z.B. betreffend Selbstregulierung, Organisation des Handels sowie Vor- und Nachhandelstransparenz[468] einzuhalten (Art. 73b FinfraG[469]), die regelmässig auch Informationspflichten mitbeinhalten.

Weiter im Blickfeld zu behalten ist die Anordnung von Art. 73d Abs. 3 FinfraG, die dem Bundesrat die Kompetenz einräumt, Mindestanforderungen an das Register zu erlassen (lit. a), und zwar insbesondere im Interesse der Integrität und der Publizität der DLT-Handelsplattform. Die Konkretisierung erfolgt in Art. 58g FinfraV: Demnach können DLT-Effekten vom DLT-Handelssystem zugelassen werden, wenn das verteilte elektronische Register mindestens die Anforderungen nach Art. 973d Abs. 2 OR erfüllt,[470] und damit eine technikbezogene Parallelität eintritt. Zusätzliche Informationspflichten sind damit aber nicht verbunden.

b) Haftungsfolgen

Der aktivlegitimierte Ersterwerber oder spätere Erwerber kann gegen den Betreiber des Wertrechteregisters (und ggf. der DLT-Handelsplattform) vorgehen. Die Erweiterung der Passivlegitimation auf alle Personen, die in massgeb-

467 Im Einzelnen dazu *Kuhn*, 2021a, Rz. 168 m.w.V.

468 Eingehend dazu nun *Humbel*, 2019, 1 ff.

469 Dazu Botschaft DLT-Gesetz, BBl 2020, 312; vgl. auch Kap. III.C.1.d) und III.C.5.a).

470 Vgl. auch Kap. III.C.2.b)bb).

licher Weise an der Begebungstransaktion mitgewirkt haben (entsprechend der Prospekthaftpflicht), findet in Art. 973i Abs. 2 OR keine Stütze. Diese Einengung in einem sehr technischen Bereich ist nicht unproblematisch.[471]

Im Übrigen sind die Kriterien der Pflichtverletzung, des Schadens, des adäquaten Kausalzusammenhangs und des Verschuldens (im Vertragskontext mit Beweislastumkehr) zu erfüllen.

[471] Vgl. dazu *Kuhn*, 2021a, Rz. 172.

VI. Alternative Streitschlichtung

Trotz der Automatisierung und Risikominderung auf DLT-Systemen sind auch die Streitschlichtungsmechanismen[472] im Rahmen der DLT zu untersuchen, da sich bei der Verwendung von DLT-Infrastrukturen, insbesondere bei der Verwendung von Smart Contracts, durchaus Probleme bei Transaktionsabwicklungen ergeben können. In einem solchen Fall werden die staatlichen Gerichte oft als nicht effizient genug angesehen; aus diesem Grund sind insbesondere Alternative-Dispute-Resolution-Lösungen (ADR-Lösungen) von grosser Bedeutung.[473]

Gesetzliche Regeln für Streitbeilegungsmechanismen mit Blick auf DLT-Handelsplattformen sind bisher nicht vorhanden. Angesichts der Interessen des Wirtschaftsstandortes Schweiz besteht ein Handlungsbedarf, eine attraktive Lösung für Streiterledigungsverfahren zu finden. Nachfolgend werden die Entwicklungen im Bereich des Finanzmarkts bzgl. ADR (A.) und die Weiterentwicklung zu potenziellen Ausgestaltungen der On-Chain Dispute Resolution aufgearbeitet (B.), bevor sie auf ihre Tauglichkeit für DLT-Handelsplattformen hin überprüft werden (C.).

A. Dispute Resolution auf Finanzmärkten

In Bezug auf ADR existieren insbesondere in Finanzmärkten unterschiedliche Ansätze im internationalen Vergleich. Um mit Blick auf die Diskussion der alternativen Streitschlichtung auf DLT-Systemen eine möglichst breite Auslegeordnung zu erhalten, thematisiert dieses Kapitel vorerst die vielfältigen ADR-

472 Das Schrifttum spricht in der Regel von *Alternative Dispute Resolution* (ADR); hernach werden grundsätzlich die englischen Begriffe verwendet, weil sie in der Literatur gebräuchlicher sind.

473 Der nachfolgende Text basiert in den Grundzügen auf *Rolf H. Weber/Okan Yildiz*, Alternative Dispute Resolution auf DLT-Handelsplattformen. In: Jusletter 14. Juni 2021 und wurde mit den neusten Entwicklungen und Erkenntnissen ergänzt; dieser Beitrag (*Weber/Yildiz*, 2021) wird nachfolgend nicht überall referenziert.

und die Online-Dispute-Resolution-Verfahren.[474] Im Lichte der ausländischen Ausprägungen sind das Ombudsmansystem, die Mediation und die Schiedsgerichtsbarkeit genauer zu betrachten.

1. Ombudspersonen

Systeme mit Ombudspersonen sind im Vereinigten Königreich, in Australien und in Japan verwirklicht; diese Verfahren lassen sich wie folgt zusammenfassen:

a) Vereinigtes Königreich

Im Vereinigten Königreich weist das Ombudswesen eine lange Tradition auf; es existieren verschiedene branchenspezifische Ombudsman-Verfahren. Ohnehin ist die alternative Streitbeilegung im Vereinigten Königreich bereits seit langer Zeit in die britische Zivilprozessordnung eingeflossen.[475]

Für den Finanzmarkt besteht der Financial Ombudsman Service (FOS). Das Ziel des FOS ist es, die Position der wirtschaftlich schwächeren Kundinnen und Kunden gegenüber den Finanzinstituten zu stärken. Der FOS bietet deshalb seine Dienstleistungen für Private und kleinere Unternehmen kostenlos an und gibt eine Empfehlung ab, welche indessen in einem allfälligen ordentlichen Verfahren keine Wirkung entfaltet.[476] Nach gesetzlicher Vorgabe wird der FOS durch Abgaben und Fallpauschalen getragen. In der Regel haben die Kundinnen und Kunden sich zuerst an das Finanzinstitut zu wenden; sie können bereits in diesem Schritt um Unterstützung bitten.[477]

Die Beschwerden werden am häufigsten einvernehmlich zum Abschluss gebracht;[478] können sich die Parteien nicht einigen, entscheidet ein Ombudsman den Fall ohne Ansetzung eines Termins. Ein von den Kundinnen und Kunden

---

474 Für einen Überblick zur Entwicklung der ODR-Verfahren und einer Umsetzungsmöglichkeit in der Europäischen Union, vgl. *Weber/Yildiz*, 2021, Rz. 5 ff.

475 *Weber/Baisch*, 2015, 781 m.w.V.

476 Detaillierte Informationen zum FOS sind zu finden unter <https://www.handbook.fca.org.uk/handbook/DISP.pdf>.

477 *Weber/Baisch*, 2015, 781 f.

478 Die Financial Conduct Authority (FCA) führt und veröffentlich detaillierte Daten zu den Beschwerden beim FOS, vgl. FCA, Complaints data, aufrufbar unter <https://www.fca.org.uk/data/complaints-data> und zu den Gesamtdaten für das zweite Halbjahr 2021, vgl. FCA, Aggregate complaints data: 2021 H2, aufrufbar unter <https://www.fca.org.uk/data/complaints-data/aggregate-complaints-data-2021-h2>.

akzeptierter Entscheid bis zur Obergrenze von 375'000 £ (ca. 435'000 CHF) ist für die Finanzinstitute bindend.[479] Sollten die Kundinnen und Kunden nicht zufrieden sein mit der Entscheidung des Ombudsman, können sie den Fall an ein Gericht weiterziehen.[480]

b) Australien

Auch in Australien ist die aussergerichtliche Streitbeilegung über einen Ombudsman gängig. Neben staatlichen Ombudsstellen haben sich branchenbezogene Ombudsstellen bewährt; als Beispiele für Industriezweige mit Ombudsstellen lassen sich der Energiesektor, der Telekommunikationssektor und der Finanzsektor erwähnen.[481]

In Australien sind die Finanzinstitute verpflichtet, interne Beschwerdemöglichkeiten einzuführen, um Streitigkeiten mit den Kundinnen und Kunden systematisch abwickeln zu können. Führen diese internen Beschwerdemöglichkeiten zu keinem Ergebnis, bestehen externe Streitschlichtungsstellen (engl. External Dispute Resolution [EDR]).[482] Im Jahre 2018 hat die Australian Financial Complaints Authority (AFCA) die Vorgängerinfrastruktur, nämlich den Financial Ombudsman Service (FOS), den Credit and Investments Ombudsman (CIO) und das Superannuation Complaints Tribunal (SCT), abgelöst. Die Details der AFCA-Verfahren sind in den AFCA Rules geregelt.[483]

Die AFCA schlichtet zwischen Verbraucherinnen und Verbrauchern sowie den Finanzinstituten, die Mitglied der AFCA sind; hierfür reichen die Verbraucherinnen und Verbraucher eine Beschwerde über ein Online-Formular, telefonisch oder mit einem Schreiben ein. Die AFCA benutzt in erster Linie informelle Methoden zur Streitschlichtung, wie z.B. die Vermittlung von Verhandlungen. Führen die informellen Verhandlungen zu keinem Ergebnis, kann das Beschwerdeverfahren weitergeführt werden; dabei gibt die AFCA eine Recommendation ab. Falls die Parteien die Recommendation nicht anerkennen, verfügt ein AFCA-Entscheidungsträger eine Determination. Diese kann

479 Für die Obergrenze, vgl. Sec. 3.7.4 des Handbook zu «Dispute resolution: Complaints», aufrufbar unter <https://www.handbook.fca.org.uk/handbook/DISP.pdf>.

480 Vgl. FOS, How to complain, aufrufbar unter <https://www.financial-ombudsman.org.uk/consumers/how-to-complain>.

481 *Ali*, 2013, 64 f.

482 *Ali*, 2013, 67.

483 Australian Financial Complaints Authority (AFCA), Complaint Resolution Scheme Rules vom 13. Januar 2021.

nur durch die Verbraucherseite vor ein ordentliches Gericht gezogen werden (sec. A 15). Die durch die AFCA erlangten Informationen haben in allfälligen nachfolgenden Gerichtsverfahren keine Wirkungen bzw. sie dürfen nicht verwendet werden, ausser wenn das Gericht dies ausdrücklich verlangt (sec. A 11.1; sec. A 11.2 mit den Ausnahmen).

c) Japan

Obwohl in der japanischen Rechtsordnung die ADR-Möglichkeiten nicht so stark entwickelt sind, gibt es Dispute Resolution Organisationen für die Finanzmärkte, welche die japanische Finanzaufsichtsbehörde als Designated Dispute Resolution Organizations (Art. 156-38 FIEA[484]) anerkennt. Die Finanzinstitute sind gemäss Art. 37-7 FIEA verpflichtet, einen Rahmenvertrag über die Durchführung von Beschwerden und Streitbeilegungsverfahren mit einer solchen Designated Dispute Resolution Organization einzugehen. Es ist den Finanzinstituten überlassen, sich einer Designated Dispute Resolution Organization anzuschliessen; sie sind aber nicht verpflichtet, an einem Verfahren teilzunehmen, falls die Kundinnen und Kunden sich an eine andere Designated Dispute Resolution Organization als jener, die mit dem Finanzinstitut eine Vertragsbeziehung hat, wenden. Als Beispiel einer Designated Dispute Resolution Organization ist die Financial Instruments Mediation Assistance Center (FINMAC) zu nennen, welche den Eindruck einer gewissen Unabhängigkeit vermittelt.[485]

Die Designated Dispute Resolution Organizations sind gehalten, innerhalb des gesetzlichen Rahmens eigene Regeln aufzustellen, wie z.B. Regeln, welche für die Bearbeitung von Beschwerden über die Streitbeilegungsdienste relevant sind (Art. 156-44 Abs. 1 [vii]). Die gesetzliche Vorgabe in Art. 156-60 (6) zeigt, dass neben einem internen Einigungsvorschlag auch eine abschliessende Beurteilung der Streitsache möglich ist («A *Dispute Resolution Mediator may […] prepare the settlement proposal that is needed to resolve the case and recommend that the Parties accept it, or implement a special conciliation*»).

484 Financial Instruments and Exchange Act, Act No. 25 of April 13, 1948 (englische Übersetzung aufrufbar unter <https://www.japaneselawtranslation.go.jp/en/laws/view/2355/en>).

485 *Weber/Baisch*, 2015, 785 f.

2. Mediation/Schiedsgerichtsbarkeit

Neben der Streitbeilegung gestützt auf das System des Ombudsman kennen einige wichtige Finanzplätze (Hong Kong, Singapur, die Vereinigten Staaten von Amerika und China) die Mediation und/oder die Schiedsgerichtsbarkeit.

a) Hong Kong

In Hong Kong bearbeitet das Financial Dispute Resolution Centre (FDRC) kleinere Streitigkeiten bis 1'000'000 HK$ (ca. 120'000 CHF).[486] Die Parteien können ihre Streitigkeit zunächst in einem kostengünstigen Mediationsverfahren, bei dem die klagende Partei die Application Fee zu zahlen hat, lösen. Finden sie keine Einigung, besteht die Möglichkeit, ein grundsätzlich dokumentenbasiertes Schiedsverfahren (mit Zahlung der Arbitration Fees) durchzuführen.[487]

Positiv auffallend sind die kurzen Fristen im Verfahren des FDRC. Bei der Mediation sind – mit Ausnahme der Extended Eligible Disputes – auf beiden Seiten keine Legal Representatives (oder In-House Lawyers) zugelassen (sec. 2.3.3). Zudem unterstützt auch die Gebührenstruktur eine Einigung, denn Klagende haben je nach Höhe des Streitwerts 1'000 bzw. 2'000 HK$ (ca. 120-250 CHF) zu zahlen, während die Finanzinstitute 5'000 bzw. 10'000 HK$ (ca. 600-1'200 CHF) zu zahlen haben; auch der Weiterzug an die Schiedsgerichtsbarkeit zeigt eine ähnliche Struktur, denn die Klagenden haben dort 5'000 HK$ (ca. 600 CHF) und die Finanzinstitute 20'000 HK$ (ca. 2'400 CHF) einzuschiessen.[488] Dass diese Verfahren auf eine Einigung abzielen, zeigt sich auch am Umstand, dass selbst beim Schiedsverfahren keine Legal Representatives (oder In-House Lawyers) zugelassen sind (sec. 3.8.3 [c]). Der Schiedsspruch ist an sich final, jedoch bestehen vereinzelte Möglichkeiten, diesen noch anzufechten (vgl. den Verweis auf die Arbitration Ordinance in sec. 3.12.1).

---

486 Vgl. Terms of Reference for Financial Dispute Resolution Centre (FDRC) in relation to the Financial Dispute Resolution Scheme (FDRS), November 2018 Revision.

487 Vgl. auch *Weber/Baisch*, 2015, 786 f.

488 Financial Dispute Resolution Centre (FDRC), Fees - For Cases of Standard Eligible Dispute under Terms of Reference (Jan 2018), aufrufbar unter <https://www.fdrc.org.hk/en/html/resolvingdisputes/resolvingdisputes_scheduleoffees.php>.

b) Singapur

In Singapur gibt es seit 2005 das Financial Industry Dispute Resolution Centre (FIDReC), welches in einem ersten Schritt die Schlichtung über die Mediation und in einem zweiten Schritt die Verfahrenserledigung durch die Schiedsgerichtsbarkeit vorschreibt.

Die Streitbeilegung des FIDReC gliedert sich grundsätzlich in drei Instanzen, nach denen sich die Kundenbeschwerden im Finanzdienstleistungsbereich beilegen lassen. Nach dem Counseling Service können die Parteien eine förmliche Beschwerde beim Case Manager (Mediator) einreichen. Vermag der Case Manager nicht erfolgreich zu vermitteln, übernehmen zugelassene Schiedsrichter den Fall; die Finanzinstitute sind an den Entscheid des Schiedsgerichts gebunden, während die Kundinnen und Kunden den Rechtsweg einschlagen können. Die Entscheide beim FIDReC haben somit für die Kundinnen und Kunden keine präjudizielle Wirkung.[489]

Die Finanzierung der FIDReC erfolgt fast ausschliesslich über die Finanzindustrie; die Kundinnen und Kunden müssen bloss eine Schutzgebühr zahlen, falls die Mediation nicht gelingt und ein Schiedsverfahren erforderlich wird.[490]

c) Vereinigte Staaten von Amerika

In den Vereinigten Staaten stehen mehrere Stellen für Mediation und/oder Schiedsgerichtsbarkeit zur Verfügung;[491] die bekannteste Organisation ist die Financial Industry Regulatory Authority (FINRA). Im Fokus der FINRA liegt neben der schnellen, effizienten, unparteiischen und relativ preiswerten auch die finale Erledigung der Streitsache, jedoch muss bei langandauernden Verfahren mit erhöhten Gebühren gerechnet werden.

Das Modell in den USA zeigt gewisse Probleme gut auf, denn es beabsichtigt die Kundinnen und Kunden vor unfairen Schiedsklauseln zu schützen und will trotzdem, dass kundenfreundliche ADR-Angebote auch ohne vertragliche Regelung allen offenstehen. Gesetzlich ermächtigt sec. 921 des Dodd–Frank Wall

489 *Weber/Baisch*, 2015, 787 f.

490 *Weber/Baisch*, 2015, 788.

491 Vgl. *Gut*, 2014, 163 ff.; *Ali*, 2013, 111.

Street Reform and Consumer Protection Act[492] die Securities and Exchange Commission (SEC), Schiedsvereinbarungen in den Kundenverträgen zu untersagen, um die Kundinnen und Kunden vor unfairen Schiedsklauseln zu schützen. Indessen steht ihnen das ADR-Verfahren der FINRA zur Verfügung, selbst wenn dies nicht vertraglich geregelt worden ist; sie bleiben frei, zunächst das unverbindliche Mediationsprogramm anzurufen oder direkt ein Schiedsverfahren einzuleiten.[493]

In den USA ist die American Arbitration Association (AAA) eine der bekanntesten alternativen Streitbeilegungsinstitutionen; die AAA bietet auf Grundlage der AAA Arbitration Rules for Commercial Financial Disputes[494] ihre Dienste für alle Arten von Finanzstreitigkeiten an.

d) China

Zu den bevorzugten Methoden der Streitschlichtung im Finanz- und Handelsbereich gehört in China die Schiedsgerichtsbarkeit; sowohl die China International Economic and Trade Arbitration Commission (CIETAC) als auch die Provinz- und Ortsgerichte (einschliesslich der Gerichte in Shanghai) haben spezielle Streitschlichtungsverfahren zur Beilegung von Handels- und Finanzstreitigkeiten entwickelt. Da die Ad-Hoc-Schiedsgerichtsbarkeit in China bei Sachverhalten innerhalb von China nicht erlaubt ist, ist über eine offiziell anerkannte Institution ein institutionelles Schiedsgerichtsverfahren durchzuführen. Ein Ergebnis dieser Regelung ist, dass die Parteien bei der Wahl Chinas als Ort des Schiedsverfahrens in der Auswahl der verfahrens- und materiellrechtlichen Vorschiften eingeschränkt sind.[495]

Die CIETAC hat im Jahre 2003 die China International Economic and Trade Arbitration Commission Financial Disputes Arbitration Rules[496] erlassen, die im

---

492 An Act to promote the financial stability of the United States by improving accountability and transparency in the financial system, to end «too big to fail», to protect the American taxpayer by ending bailouts, to protect consumers from abusive financial services practices, and for other purposes, Pub.L. 111–203, 124 Stat. 1376–2223.

493 *Weber/Baisch*, 2015, 789 m.w.V.

494 American Arbitration Association (AAA), Arbitration Rules for Commercial Financial Disputes, effective June 1, 2009.

495 *Ali/Huang*, 2012, 86 m.w.V.

496 CIETAC Financial Disputes Arbitration Rules-China International Economic and Trade Arbitration Commission (Revised and Adopted by the China Council for the Promotion of International Trade/China Chamber of International Commerce on November 4, 2014. Effective as from January 1, 2015).

Jahre 2014 revidiert wurden; diese Rules regeln die Schiedsverfahren im Finanzbereich. Seit 1985 ist in der Zahl der bearbeiteten Fälle durch die CIETAC ein konstanter Anstieg zu erkennen; im Jahr 2021 bearbeitete die CIETAC 4071 Fälle.[497]

Neben der bereits erwähnten CIETAC hat auch das durch die Shanghai International Economic and Trade Arbitration Commission eingerichtete Shanghai International Arbitration Center (SHIAC), welches seit 2017 eine stetige Erhöhung der Fallzahlen aufweist,[498] eine grosse Bedeutung in China erlangt; die Verfahren wenden die SHIAC-Rules an.[499] In Fällen bis zu einer Obergrenze von 1'000'000 ¥ (ca. 7'000 CHF) wird im summarischen Verfahren mit einem einzigen Schiedsrichter bzw. Schiedsrichterin entschieden, ausser die Parteien einigen sich auf gegenteilige Regelungen (Art. 52/53 SHIAC-Rules).

B. Neue Formen der Dispute Resolution

Wie dargelegt, kennen die untersuchten Länder verschiedene ADR-Ansätze im Rahmen von Streitigkeiten auf den Finanzmärkten. Diese ausgeprägte Kultur von ADR auf Finanzmärkten, welche bereits viele Erfahrungswerte einbringt, kann als Grundlage dienen, um neuen Formen der Dispute Resolution eine Plattform zu bieten.

Im Rahmen der Digitalisierung entwickelten sich verschiedene «Online Dispute Resolution»-Ansätze (ODR-Ansätze). Bereits im Jahre 1999 begann eBay mit einem ersten Test für ein ODR-Verfahren. Etwa 17 Jahre später hat die Europäische Union ebenfalls eine ODR-Plattform in Betrieb genommen. Die UNCITRAL hielt in einem Report zur Online Dispute Resolution[500] fest, dass es für internationale Online-Transaktionen ein spezielles Verfahren brauche, um entstehende Streitigkeiten zu erledigen.

---

497 *China International Economic and Trade Arbitration Commission*, CIETAC Annual Caseload (Foreign-Related and Domestic), aufrufbar unter <http://www.cietac.org/index.php?m=Page&a=index&id=40&l=en>.

498 *Shanghai International Economic and Trade Arbitration Commission*, *Shanghai International Arbitration Center*, SHIAC Annual Report 2021, aufrufbar unter <http://www.shiac.org/shiac/news_detail_E.aspx?id=1991>.

499 *Shanghai International Economic and Trade Arbitration Commission*, *Shanghai International Arbitration Center*, Arbitration Rules, effective as from January 1, 2015.

500 UNCITRAL, Report of Working Group III (Online Dispute Resolution) on the work of its thirty-third session (New York, 29 February-4 March 2016), A/CN.9/868.

Durch die Fortschritte im Bereich der DLT haben sich neue Möglichkeiten entwickelt, Streitbeilegungsmethoden weiter zu automatisieren. Oft stehen aber Projekte mit einer vollumfänglichen Automatisierung der Streitbeilegung erst in der Pilotphase oder konnten sich noch nicht durchsetzen. Die Verfahren im Bereich der Off-Chain und/oder der On-Chain Dispute Resolution hingegen scheinen realisierbar zu sein. Besonders zu analysieren ist, inwieweit der Aufbau der DLT sowie die angestrebte Dezentralität und Pseudonymität mit den Grundsätzen der Schiedsgerichtsbarkeit vereinbar sind.

1. Online Dispute Resolution (ODR)

Seit Beginn der Verbreitung von E-Commerce-Plattformen gibt es einen Bedarf für alternative Streitbeilegungsmethoden. Aufgrund der grösseren Flexibilität konnten die privaten Unternehmen relativ kurzfristig ihre eigenen, zentralen Dispute Resolution-Verfahren einrichten (z.B. eBay, PayPal, Amazon). Auch staatliche Institutionen haben den Bedarf erkannt; so hat die EU im Jahre 2016 die Consumer ODR-Plattform geschaffen. Die nachfolgenden Ausführungen stellen verschiedene ODR-Verfahren vor.

a) Dispute Resolution Center von eBay

Bereits im März 1999 hat eBay einen versteckten Link auf ihrer Website hinterlegt, welcher den Nutzenden erlaubte, eine Beschwerde einzureichen für Streitigkeiten, die bei einer Transaktion auf ihrer Website entstanden sind. Obwohl der Link versteckt war, haben in den ersten zwei Wochen 225 Nutzerinnen und Nutzer dieses Verfahren beansprucht. Diese Vorgängerversion eines ODR-Verfahrens sah einen Mediator als Schlichtungsstelle vor, welcher manuell die Käuferinnen und Käufer sowie Verkäuferinnen und Verkäufer per Mail kontaktierte und durch Mediation eine Lösung weiterzuführen versuchte.[501] Heute ist das Dispute Resolution Center von eBay eines der weltweit grössten ODR-Systeme und führt jährlich schätzungsweise mehr als 60 Millionen E-Commerce Disputes durch.[502]

Das ODR-Verfahren von eBay beschränkt sich auf die Rückzahlung des Preises (Käuferseite) und die Rückerstattung der Ware (Verkäuferseite); Schadenersatzansprüche können beim Dispute Resolution Center nicht geltend gemacht werden.

501 Vgl. *Katsch/Rifkin/Gaitenby*, 2000, 709 f.

502 *Del Duca/Rule/Rimpfel*, 2014, 205.

Das ODR-Verfahren von eBay wird zusammen mit PayPal verwaltet. In einem ersten Schritt geben die Käuferinnen und Käufer die Besonderheiten ihrer Beschwerde an und schlagen eine bevorzugte Lösung vor. In einem nächsten Schritt animiert eBay automatisch die Käuferinnen und Käufer sowie Verkäuferinnen und Verkäufer, durch bilaterale Verhandlungen eine Lösung zu finden. Kommt es zu keiner Lösung, können die Parteien das Dispute Resolution Center von eBay anrufen. Auf der Plattform stehen verschiedene Optionen zur Auswahl.[503] Das Verfahren ist vollständig automatisiert; ein Eingriff durch einen Menschen ist nur erforderlich, wenn die Käuferseite sich gegen einen sog. «Unpaid Item Strike» beschwert (z.B. mit der Behauptung, dass er/sie kein Angebot abgab oder bereits bezahlt habe). Mit dieser Lösung können mehrere Millionen ODR-Verfahren vollautomatisiert abgeschlossen werden, während nur wenige zehntausend Anfechtungen einer menschlichen Überprüfung bedürfen.

b) Consumer ODR in der EU

Seit dem 15. Februar 2016 ist die Europäische Plattform für Online-Streitbeilegung (OS-Plattform) in Betrieb; die Verordnung (EU) Nr. 524/2013[504] musste dazu mit der Durchführungsverordnung (EU) 2015/1051[505] der Kommission ergänzt werden. Im ersten Jahr zählte die Plattform über 24'000 Beschwerden von Verbraucherinnen und Verbrauchern.[506] Die Verordnung gilt für Streitigkeiten aus Online-Kauf- oder Online-Dienstleistungsverträgen zwischen Verbraucherinnen und Verbrauchern und Unternehmern, welche unter die Richtlinie 2013/11/EU[507] fallen (Art. 2 Abs. 1 ODR-Verordnung).

---

503 Als Beispiele sind Auswahlmöglichkeiten wie «Ich habe den Artikel noch nicht erhalten.» oder «Ich habe mein Geld noch nicht erhalten.» zu nennen.

504 Verordnung (EU) Nr. 524/2013 des Europäischen Parlamentes und des Rates über die Online-Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG vom 21. Mai 2013, ABl. L 165, 1–12.

505 Durchführungsverordnung (EU) 2015/1051 der Kommission über die Modalitäten für die Ausübung der Funktionen der Plattform zur Online-Streitbeilegung, über die Modalitäten des elektronischen Beschwerdeformulars und die Modalitäten der Zusammenarbeit der Kontaktstellen gemäss der Verordnung (EU) Nr. 524/2013 des Europäischen Parlaments und des Rates über die Online-Beilegung verbraucherrechtlicher Streitigkeiten vom 1. Juli 2015, ABl. L 171, 1–4.

506 Online-Handel und Online-Streitbeilegung (OS): 24 000 Verbraucher nutzten die neue europäische Plattform im ersten Jahr, Pressemitteilung der Kommission vom 27. März 2017, aufrufbar unter <https://ec.europa.eu/commission/presscorner/detail/de/IP_17_727>.

507 Richtlinie 2013/11/EU des Europäischen Parlamentes und des Rates über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG vom 21. Mai 2013, ABl. L 165, 63–79.

Die Verordnung verpflichtet in der Union niedergelassene Unternehmer, die Online-Kauf- oder Dienstleistungsverträge eingehen, einen Link zur OS-Plattform zur Verfügung zu stellen (Art. 14 Abs. 1 ODR-Verordnung), um den Zugang für Verbraucherinnen und Verbraucher auf das ODR-Verfahren zu erleichtern; die Plattform ist in allen EU-Sprachen verfügbar. Zudem sind die Mitgliedstaaten gehalten, mindestens eine Kontaktstelle für die OS-Plattform zu benennen, welche die Beilegung der Streitigkeiten unterstützt (Art. 7 ODR-Verordnung).

Das ODR-Verfahren in der EU funktioniert ähnlich wie das Verfahren von eBay. Die OS-Plattform als zentrale Anlaufstelle erleichtert den Einstieg für Verbraucherinnen und Verbraucher, um ihre Rechte geltend zu machen. Die Verbraucherseite muss auf der OS-Plattform der EU ein elektronisches Beschwerdeformular ausfüllen; sie kann anklicken, was sie bereits unternommen hat und worum es beim Konflikt geht.[508] Die OS-Plattform setzt hernach die Unternehmerseite automatisch über das Ersuchen der Verbraucherseite in Kenntnis. Die Parteien können sich direkt über die Plattform austauschen (z.B. mit Nachrichten oder Bildern des Produkts). Sie haben 90 Tage Zeit, um auf der Plattform eine Lösung zu finden. Kommt es nicht dazu oder möchte das Unternehmen nicht verhandeln, sucht die Plattform eine Streitbeilegungsstelle, welche das Verfahren online fortsetzt. Die OS-Plattform übermittelt dieser alle Informationen und versorgt die Parteien ggf. mit Übersetzungen. Finden die Parteien eine Lösung, kann das Verfahren auf der OS-Plattform abgeschlossen werden, ansonsten steht der Weg zu den Europäischen Verbraucherzentren oder staatlichen Gerichten offen.

Die OS-Plattform dient somit als zentrale Vermittlerin beider Seiten, welche mit automatisierten Prozessen auch das Verfahren ausserhalb der Plattform (z.B. bei einer Streitbeilegungsstelle) erleichtert. Jedoch liegt kein vollautomatisierter Prozess vor, weil Dritte zur Lösungsfindung eingeschaltet werden müssen. Das System basiert zudem auf Freiwilligkeit; die Unternehmen können sich querstellen, indem sie nicht auf Verhandlungen eingehen und somit den Weg über ein staatliches Gericht provozieren. Dennoch ermöglicht die Plattform den ersten Schritt zu einer potenziellen Streitbeilegung und sie kann als Leitfaden für die nächsten Schritte der Verbraucherseite dienen.

[508] Zum Beispiel «Kontaktaufnahme mit dem Unternehmer» bzw. «Waren oder Dienstleistungen im Wert von über 5'000 EUR».

Zusätzlich zu dieser OS-Plattform beabsichtigt die EU, künftig den Güter und Dienstleistungen anbietenden Online-Plattformen vorzuschreiben, mittels eines Vermittlungsdienstes ein internes Beschwerdemanagementsystem mit anschliessender aussergerichtlicher Streitbeilegung einzuführen (Art. 17/18 der E-DSA); das Gesetzgebungsvorhaben dürfte aber noch einige Zeit in Anspruch nehmen.[509]

2. On-Chain Arbitration

a) Einleitung

Die DLT dient als technische Grundlage für die Ausführung von Smart Contracts;[510] diese Tatsache eröffnet verschiedene Möglichkeiten für den Einsatz von On-Chain Arbitration. Der Begriff On-Chain Arbitration ist nicht ganz präzis, weil das Schiedsverfahren selbst (abgesehen von potenziellen Ausprägungen der AI-powered oder Crowdsourced Schiedsverfahren) ausserhalb der betroffenen Chain stattfindet; alle anderen Vorgänge werden aber auf der Blockchain abgebildet (der Smart Contract basiert auf der Blockchain und der Schiedsspruch kann auf der Blockchain ausgeführt und vollzogen werden); deshalb wird der Begriff On-Chain Arbitration verwendet. In der Literatur existiert auch der Begriff Off-Chain Arbitration, jedoch handelt es sich dabei nicht um eine spezifische Ausprägung der Schiedsgerichtsbarkeit, sondern vielmehr um «traditionelle» Schiedsverfahren, die sich insbesondere auf die Besonderheiten der DLT konzentrieren. Diese Schiedsverfahren basieren in der Regel auf den Grundlagen der bereits existierenden institutionellen Schiedsgerichte, können aber die speziellen Arbitration Rules (z.B. JAMS[511] oder DDRR[512]) für die DLT miteinbeziehen.[513]

---

509 Zum Entwurf vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG vom 15. Dezember 2020, COM/2020/825 final; vgl. für erste Lesung die Website des Europäischen Parlaments, aufrufbar unter <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_DE.html>.

510 Für weiterführende Hinweise dazu vgl. Kap. II.B.5; vgl. auch *Weber*, 2018a, 292 ff.

511 JAMS, JAMS Rules Governing Disputes Arising out of Smart Contracts, aufrufbar unter <https://www.jamsadr.com/rules-smart-contracts>.

512 UK Jurisdiction Taskforce of Lawtech, Digital Dispute Resolution Rules, aufrufbar unter <https://lawtechuk.io/explore/ukjt-digital-disputes-rules>.

513 *Scott/Brown/Flakoll/Ossio*, 2022, 4 f. Da es sich bei diesem Verständnis der Off-Chain Arbitration nicht um eine neue Art und Weise der Ausgestaltung des Schiedsverfahrens handelt, wird diese Variante nachfolgend nicht weiter verfolgt.

Die Bedeutung der On-Chain Arbitration ist nicht zu unterschätzen, denn auch im Falle der Verwendung von Smart Contracts können sich verschiedene Probleme im Rahmen der Verfahrenserledigung durch staatliche Gerichte ergeben. Angesichts der dezentralisierten, teils anonymisierten Parteien ist bereits die Zuständigkeit der Gerichte eine komplizierte Angelegenheit.[514] Darüber hinaus ist zu prüfen, welche bzw. ob eine Rechtsordnung die Smart Contracts regelt.[515] Sind erst einmal die Jurisdiktion und das anwendbare Recht geklärt, stellt sich weiter die Frage, ob ein getroffener Entscheid auch effektiv durchsetzbar ist.[516]

b) Grundlagen der On-Chain Arbitration

Der Grundgedanke, eine Art On-Chain Arbitration bzw. einen On-Chain Streitbeilegungsmechanismus zum Schutz der Käuferinnen und Käufer zur Verfügung zu stellen, kann aus dem Whitepaper der Bitcoin abgeleitet werden.[517] Ein wichtiger Vorteil der Smart Contracts besteht darin, dass auf der einen Seite Vermögenswerte als mögliche Leistung bei einer allfälligen Vertragsverletzung bzw. als Vorschuss für das Schiedsverfahren und auf der anderen Seite auch Dokumente als mögliche Beweismaterialien bereits im Voraus auf der Blockchain gespeichert werden können.[518] Die Parteien müssten dem Smart Contract die Erlaubnis geben, die Vermögenswerte und Dokumente an ein Schiedsgericht bzw. nach dem Entscheid des Schiedsgerichts an die andere Partei zu übermitteln. Mit der Einleitung des Schiedsverfahrens können alle nötigen Dokumente ohne Weiteres dem Schiedsgericht zur Verfügung gestellt werden. Sobald das Schiedsgericht als letzte Instanz einen Entscheid gefällt hat, lässt sich der Smart Contract benachrichtigen, die Vermögenswerte an die berechtigte Partei zu übertragen. Alternativ besteht die Möglichkeit, relevante Dokumente oder Beweismittel nachzureichen.[519]

---

514 *Scott/Brown/Flakoll/Ossio*, 2022, 2 f.; *Landbrecht/Wehowsky*, 2022, 315; *Chevalier*, 2021, 561 ff.; *von Rosenstiel*, 2021, 271; *Schmitz/Rule*, 2019, 105 m.w.H.; *Kaal/Calcaterra*, 2017, 127 ff.

515 *Scott/Brown/Flakoll/Ossio*, 2022, 2 f.

516 *Kaal/Calcaterra*, 2017, 137 f.; *O'Shields*, 2017, 187; zur Herausforderung der Umsetzung von On-Chain Arbitration bzw. Blockchain Arbitration, vgl. *Chevalier*, 2021, 567 ff.

517 *Nakamoto*, 2008, 1 («[…] and routine escrow mechanisms could easily be implemented to protect buyers»).

518 Denkbar ist bspw. die Implementierung einer allenfalls angepassten Sequestration; ähnlich auch *Werbach/Cornell*, 2017, 344 f.; vgl. auch *Scott/Brown/Flakoll/Ossio*, 2022, 6; *Palombo/Battaglini/Cantisani*, 2021, 128; vgl. zur Speicherung von Dokumenten auf der Blockchain Kap. II.C.3.a).

519 Vgl. *Schmitz/Rule*, 2019, 108; *O'Shields*, 2017, 180 f.

Um eine Streitigkeit den staatlichen Gerichten zu entziehen, braucht es zunächst eine Schiedsvereinbarung. Bereits hier stellen sich erste Probleme: Sowohl die ZPO als auch das IPRG verlangen für Schiedsvereinbarungen die Textform (Art. 358 ZPO und Art. 178 Abs. 1 IPRG).[520] Demnach muss die Schiedsvereinbarung in «visuell wahrnehmbarer, physisch reproduzierbarer Form»[521] beim Empfänger eintreffen. Da die Vertragsparteien grundsätzlich weder Zugriff auf die Codierung des Vertrags haben noch die kodierte Schiedsvereinbarung in einer natürlichen Sprache vorliegt, ist erforderlich, dass ihnen der (vorangehende) Vertrag mit der Schiedsklausel (oder nur die Schiedsvereinbarung) in einer natürlichen Sprache und in «visuell wahrnehmbarer, physisch reproduzierbarer Form» zugestellt wird, bspw. mit dem Vertrag, den die Parteien zu unterzeichnen haben, um überhaupt an einem DLT-System teilnehmen zu können.[522] Alternativ gibt es in der Literatur auch Stimmen, die vorschlagen, die Schiedsvereinbarung im Smart Contract selbst zu hinterlegen.[523]

Mit Blick auf das New Yorker Übereinkommen über die Anerkennung und Vollstreckung ausländischer Schiedssprüche (NYC) zeigt sich, dass die formellen Anforderungen an die Schiedsvereinbarung strikter sein können, da Art. II Abs. 1 NYC eine schriftliche Vereinbarung (engl. *agreement in writing*) verlangt; diese Anforderung wird in der Regel von den Gerichten eng ausgelegt, weshalb eine Schiedsklausel im Smart Contract selber grundsätzlich nicht die Anforderung der schriftlichen Vereinbarung erfüllen wird.[524] Mit der (physischen) Separierung der Schiedsvereinbarung vom Smart Contract, d.h. der Aufnahme der Schiedsklausel in den Vertrag zur Nutzung eines DLT-Systems, können aber potenzielle Probleme der Konformität der Schiedsvereinbarung mit den formellen Anforderungen des NYC gelöst werden.

---

520 Der Bundesrat wollte bewusst die kürzere und modernere Formulierung des Art. 358 ZPO in Art. 178 Abs. 1 IPRG übernehmen, um die Anwenderfreundlichkeit zu stärken (vgl. Botschaft IPRG, BBl 2018, 7174).

521 BSK IPRG-*Gränicher*, Art. 178 N 24.

522 Vgl. BSK IPRG-*Gränicher*, Art. 178 N 24; vgl. ferner *Kreis/Kaulartz*, 2019, 343; *Favrod-Coune/Belet*, 2018, 1111 f.

523 *Sinitsyn/Diakonova/Chursina*, 2022, 159 f.; *Mulia/Kumari*, 2021; *Kaulartz*, 2019, 75; *Janssen/Vennmanns*, 2021, 69 f.; a.M. *Guillaume/Riva*, 2022, 43, wonach die Schiedsvereinbarung nur im Smart Contract nicht genügen darf, sondern die Parteien zusätzlich (schriftlich) zu informieren sind über potenzielle Schiedsvereinbarungen.

524 *Kreis/Kaulartz*, 2019, 343 f. m.w.V.

Die Schiedsvereinbarung ist allerdings bloss eine erste, rechtliche Voraussetzung. Ausserdem ist zu beachten, dass der Code der Smart Contracts unveränderbar und selbstausführend ist. Ein Smart Contract wird automatisch, also ohne Eingriffe von Dritten, ausgeführt und soll grundsätzlich nicht gestoppt werden können.[525] Dieser Umstand bereitet jedoch Probleme, da ein Schiedsverfahren nur zum Ziel führen kann, wenn sich die Ausführung des Smart Contract auch unterbrechen lässt. Grundsätzlich gibt es verschiedene Möglichkeiten, die Ausführung des Smart Contract aufzuhalten bzw. ein solches Schiedsverfahren zwischenzuschalten.

c) Unterbrechung des Smart Contract und Einleitung des Schiedsverfahrens

Mit Blick auf die Einleitung des Schiedsverfahrens bedürfen zwei Aspekte der besonderen Beachtung, nämlich die Smart Contract Dispute Resolution Library und die Multi-Signature-Adressen:

(i) Um effektiv auf den Ablauf des Smart Contract Einfluss nehmen zu können, ist die Einführung einer *Smart Contract Dispute Resolution Library* auf der Blockchain denkbar. Diese Bibliothek ist in den Smart Contract programmiert und kann die Transaktion bis zu einer vorbestimmten (technischen) Frist anhalten. Vor Ablauf der Frist hat der Empfänger keine Möglichkeit, über den Inhalt des Vertrags zu verfügen; während der erwähnten Frist steht es beiden Parteien frei, ein Schiedsgericht anzurufen und somit die Ausführung des Smart Contract bis zum Ende des Schiedsverfahrens aufzuhalten. Die Bibliothek könnte alle erforderlichen Dokumente und Informationen direkt an das angerufene Schiedsgericht weiterleiten.[526]

(ii) Eine andere Möglichkeit besteht darin, den Smart Contract auf *Multi-Signature-Adressen* zu gründen und noch vor seiner Durchführung anzuhalten. Das einfachste Beispiel eines Multi-Signature Smart Contract lässt sich mit der Beteiligung von drei Parteien erklären. Zur Durchführung des Smart Contract braucht es zwei der drei Schlüssel; die in der Blockchain hinterlegten Vermögenswerte werden erst übermittelt, wenn mindestens zwei Parteien der Transaktion zustimmen. Dies stellt kein Problem dar, wenn beide Parteien ihren (vertraglichen) Verpflichtungen nachgekommen sind und die Transaktion

525 *Guillaume*, 2019, 72; *Weber*, 2017c, Rz. 26.

526 *Kaulartz*, 2019, 78; zur Möglichkeit der Pausierung des Smart Contract und zum Verweis auf die Arbitration (wenn auch ohne die weitergedachte Variante der *Smart Contract Dispute Resolution Library*) vgl. *Scott/Brown/Flakoll/Ossio*, 2022, 7.

befürworten. Sobald aber eine Partei sich weigert, ihren Schlüssel bereitzustellen, muss eine dritte Person (z.B. eine Schiedsrichterin oder ein Schiedsrichter) über den Streit entscheiden und den erforderlichen zweiten Schlüssel liefern, um die Transaktion durchzuführen.[527]

Insbesondere auf kleineren DLT-Plattformen (bzw. permissioned oder privaten DLT-Systemen) ist zudem eine zusätzliche Ausgestaltung denkbar: Auf den permissioned DLT-Systemen kann bestimmten, autorisierten Teilnehmenden eine Validierungsfunktion zugeteilt werden.[528] Diese Gestaltungsmöglichkeit der DLT-Systeme würde es erlauben, dass autorisierte Teilnehmende eine Fork (eine Gabelung bzw. Bildung eines neuen Strangs) initiieren. Dadurch vermögen diese autorisierten Teilnehmenden – wohl die Betreiberinnen und Betreiber der DLT-Handelsplattformen – nach Erhalt eines (externen) Schiedsspruchs[529] ein kontrolliertes Forking durchzuführen und die strittige Transaktion zu ändern oder rückgängig zu machen.[530] In einer solchen Konstellation wäre es unerheblich, ob der Smart Contract eine Smart Contract Dispute Resolution Library implementiert, auf Multi-Signature-Adressen basiert oder bereits durchgeführt wurde und der Schiedsspruch nach Abwicklung einer Transaktion vorliegt.

d) Vollstreckung des Schiedsspruchs

In den vorgenannten Beispielen würde der Schiedsspruch selbst ausserhalb des Smart Contract gefällt werden. Jedoch zeichnen sich Smart Contracts durch ihre Unveränderbarkeit aus. Um einen solchen externen Schiedsspruch erfassen zu können, braucht es eine Schnittstelle, ein Oracle,[531] über welches der Smart Contract mit Ereignissen ausserhalb der Blockchain interagieren kann; es handelt sich also um eine externe Informationsquelle. Dieses Oracle erlaubt einem Smart Contract, die externen Informationen (der realen Welt) zu sammeln und zu speichern. Sobald der Smart Contract diese Daten benötigt, ruft der Code die erforderlichen Informationen vom Oracle ab. Erst nachdem der Smart Contract die erforderlichen Informationen – im Falle des Schiedsge-

527 *Scott/Brown/Flakoll/Ossio*, 2022, 6 f.; *Ortolani*, 2019, 434 f.; *Werbach/Cornell*, 2017, 344 f.; *Schmitz/Rule*, 2019, 123; umfassender zu Multi-Signature-Adressen vgl. *Antonopoulos*, 2017b, 149 f.; *Schär/Berentsen*, 2017, 184 f.

528 Vgl. hierzu Kap. II.A.3.

529 In dieser Variante dürfte es keine Rolle spielen, woher der Schiedsspruch stammt, solange er vollstreckbar ist.

530 Ähnlich auch *Scott/Brown/Flakoll/Ossio*, 2022, 7.

531 Vgl. zu den Oracles im Detail Kap. II.B.6.

richts den Schiedsspruch – abgerufen hat, lässt sich der Smart Contract auslösen bzw. durchführen. Das Schiedsgericht hat auf diese Weise die letztinstanzliche Autorität über die Transaktion auf der Blockchain. Auch das Oracle muss bereits im Voraus im Smart Contract programmiert sein; aus Sicherheitsgründen sollten die Parteien ein vertrauenswürdiges Oracle wählen.[532]

Oracles werden als Katalysator für On-Chain Arbitration bzw. Dispute Resolution allgemein angesehen, da sie es erlauben, menschliche Fehler ausserhalb der Blockchain («Fehler der realen Welt») in Betracht zu ziehen. Immerhin stellt diese Ausgestaltung insoweit ein zweischneidiges Schwert dar, als einerseits die Oracles es ermöglichen, dass sich überhaupt ein externer Entscheid fällen lässt und unerwünschte Folgen beseitigt werden können, sie aber andererseits in die Grundidee der Unveränderbarkeit der automatisch durchgeführten Smart Contracts eingreifen und darüber hinaus einen Single Point of Failure darstellen, der mit dem Peer-to-Peer Netzwerk der DLT abgeschafft werden sollte.

Liegt ein Schiedsspruch vor, stellt sich üblicherweise sogleich die Frage der Anerkennung und Vollstreckung, da es hierzu neben der NYC auch regionale und landesspezifische Regelungen gibt. Diese Problematik lässt sich potenziell mit der On-Chain Vollstreckung (engl. on-chain enforcement) umgehen.[533] Denkbar ist, das Schiedsverfahren bloss als Unterbrechung des Smart Contract anzusehen, sodass sich die automatische Selbstausführung des Smart Contract mit dem Empfang des Schiedsspruchs über das Oracle fortsetzt; in diesem Fall stellt das Abrufen der Informationen auf dem Oracle letztlich die «Vollstreckung» (bzw. die Fortführung des Smart Contract) dar. Da der Schiedsspruch automatisch «vollstreckt» (bzw. präziser ausgedrückt «umgesetzt») wird, braucht er auch nicht mehr in verschiedenen Ländern anerkannt

532 *Scott/Brown/Flakoll/Ossio*, 2022, 7; *von Rosenstiel*, 2021, 272; *Buchwald*, 2020, 1381 und 1383; *Allen/Lane/Poblet*, 2019, 81 f. und 87; *Ortolani*, 2019, 439; *Werbach/Cornell*, 2017, 336.

533 Trotz dieser potenziell umsetzbaren Ausgestaltungsmöglichkeit gilt es zu beachten, dass sich in dieser Variante auch Folgefragen stellen, wie z.B.: Liegt überhaupt ein Schiedsspruch vor? Falls ja, erfüllt dieser die formellen Voraussetzungen der NYC bzw. der regionalen oder landesspezifischen Regelungen? Verhindert dieser On-Chain Entscheid zukünftige Verfahren in derselben Sache?; vgl. ferner *Landbrecht/Wehowsky*, 2022, 321 f. mit einem anderen Verständnis der automatischen Vollstreckung (engl. auto-enforcement).

zu werden. Bei der Vollstreckung kann sich der Smart Contract sodann aus den Vermögenswerten auf der Blockchain bedienen; auch hier braucht es keinen Einbezug staatlicher Institutionen.[534]

C. Implementierung der ADR für DLT-Handelsplattformen

Die aufgezeigten Streitbeilegungsmechanismen basieren auf verschiedenen konzeptionellen Grundlagen, welche je nach Sachlage kombiniert und/oder gesondert benutzt werden können. Um deren Tauglichkeit für DLT-Handelsplattformen zu ermitteln, ist zunächst auf die generellen Rahmenbedingungen der Streitbeilegung einzugehen.

1. Rahmenbedingungen für ODR-Verfahren und On-Chain Arbitration

Damit die ODR-Verfahren und die On-Chain Arbitration als seriöse Schlichtungsmethoden anerkannt werden können, müssen sie selbstredend gewisse Grundsätze aufweisen und respektieren.

Bereits in Art. 1 ODR-Verordnung hält der EU-Gesetzgeber fest, dass eine Plattform einzurichten ist, «die eine unabhängige, unparteiische, transparente, effektive, schnelle und faire aussergerichtliche Online-Beilegung von Streitigkeiten» ermöglichen soll; diese Prinzipien sind für alle Arten von ODR-Verfahren zu realisieren. Insbesondere ist nicht ausser Acht zu lassen, dass jede Person bei Rechtsstreitigkeiten einen grundrechtlichen Anspruch auf Beurteilung durch eine richterliche Behörde (Art. 29a BV) sowie auf ein unabhängiges und unparteiisches Gericht (Art. 30 Abs. 1 BV) hat. Unabhängig davon, wie ein potenzielles ODR-Verfahren für Handelsplattformen ausgestaltet ist, dürfen die Nutzenden nicht gehindert werden, ihre Streitigkeit weiterhin einem ordentlichen Gericht zu unterbreiten.

Als Konkretisierungshilfe für die Einrichtung solcher Verfahren hat die UNCITRAL nicht bindende Technical Notes für ODR-Plattformen gestützt auf die

534 *Ortolani*, 2019, 435 f.; *Kaulartz*, 2019, 79 f.; vgl. ferner mit einem ähnlichen Gedankengang *Scott/Brown/Flakoll/Ossio*, 2022, 7.

Erkenntnisse ihrer Working Group III veröffentlicht.[535] Die Technical Notes sollen dazu beitragen, die Streitbeilegung in ODR-Verfahren sinnvoll zu organisieren und zu verwalten, indem sie die anwendbaren Prinzipien (Transparenz, Unabhängigkeit, Expertise), den möglichen Geltungsbereich (Section IV; «*for disputes arising out of cross-border, low-value e-commerce transactions*») oder auch Ziele und Definitionen für diese Verfahren festhalten. Die Technical Notes empfehlen insbesondere, das ODR-Verfahren in verschiedene Stufen aufzuteilen (Section III); möglich wären die (automatisierte) Verhandlung, Schlichtung, Mediation und Schiedsgerichtbarkeit.[536]

Auch die On-Chain Arbitration verlangt die Einhaltung der allgemeinen Governance-Prinzipien. Mit einer Schiedsvereinbarung können die Parteien rechtsgültig ihre Streitigkeiten der Beurteilung durch ein staatliches (d.h. gesetzlich geschaffenes) Gericht entziehen, sofern die Parteien freiwillig, unzweideutig und rechtmässig die Vereinbarung eingehen und die Mindestgarantien eines fairen Verfahrens beachten.[537] Es darf keiner Partei ein überwiegender Einfluss bei der Besetzung des Schiedsgerichts zukommen; die Schiedsrichter müssen – wie bei staatlichen Gerichten – u.a. unparteiisch und unabhängig sein. Ausserdem haben alle Schiedsverfahren die anerkannten Verfahrensgrundsätze (Gleichbehandlung der Parteien, Anspruch auf rechtliches Gehör) zu gewährleisten (vgl. Art. 373 Abs. 4 ZPO und Art. 182 Abs. 3 IPRG, Art. 190 Abs. 2 lit. d IPRG).[538] Das Schiedsverfahren verlangt nicht nur unabhängige Schiedsrichter, sondern auch die strukturelle Unabhängigkeit der Plattform.

Die zentralen Verfahrensgrundsätze sind im Dispute Resolution Kontext (vom ODR-Verfahren bis zur On-Chain Arbitration) durchgehend einzuhalten. Darüber hinaus ist es unabdingbar, ein leicht zugängliches Verfahren einzurichten, d.h. weder die Kosten für das Verfahren noch die Beweisanforderungen sollten zu hoch sein. Wie dies im Ausland bereits der Fall ist, können und sollen die (finanziell) schwächeren Parteien bevorzugt behandelt werden, indem ein Entscheid in der Anfangsphase nur für die (finanziell) stärkeren Parteien bindend ist oder indem den (finanziell) schwächeren Parteien geringere Kos-

535 Die UNCITRAL Working Group III hat von 2010–2016 an verschiedenen Sitzungen ihre Erkenntnisse zu ODR-Plattformen festgehalten und in den UNCITRAL Technical Notes on Online Dispute Resolution veröffentlicht; sie sind eine Empfehlung an alle Staaten für die Implementierung von internationalen ODR-Verfahren.

536 UNCITRAL, Technical Notes on Online Dispute Resolution, New York 2017.

537 BSK BV-*Waldmann*, Art. 29*a* Rz. 30; vgl. ferner BGE 128 III 50 E. 2 c) aa); BGE 117 Ia 166 E. 5 a).

538 *Kaufmann-Kohler/Rigozzi*, Rz. 4.108 ff. und 6.21 ff.

ten auferlegt werden.[539] Obwohl die Vertraulichkeit ein Vorteil der Schiedsgerichtsbarkeit darstellt, erscheint es als wünschenswert, dass die Verfahren transparent sind und somit der öffentlichen Kontrolle (engl. public scrutiny) unterliegen. Dies führt zu einer gewissen Berechenbarkeit der Entscheide und bietet folglich Rechtssicherheit.[540]

2. Ausgestaltungsmöglichkeiten für DLT-Handelsplattformen

Im DLT-Bericht unterscheidet der Bundesrat zwischen verschiedenen Kategorien von DLT-Handelsplattformen und greift auch – abgesehen von den schon bisher bekannten zentralen Handelsplattformen – erstmals die Unterscheidung zwischen dezentralen Handelsplattformen und Peer-to-Peer Handelsplattformen (auch distributed Handelsplattformen genannt) auf.[541] Obwohl zwischen den einzelnen Kategorien der Handelsplattformen wichtige Unterschiede betreffend der Bewilligungspflicht existieren, hat es der Bundesrat unterlassen, die Peer-to-Peer Handelsplattformen (als eine Form der alternativen DLT-Handelsplattformen) zu definieren.[542]

Die alternativen DLT-Handelsplattformen bedürfen keiner Bewilligung, weil sie unter die Schwelle des FinfraG fallen. Insbesondere Start-up-Unternehmen werden wahrscheinlich von dieser Regelung profitieren, da sie regelmässig nicht gewillt sein dürften, die gesetzlichen Anforderungen für die (de)zentralen Handelsplattformen zu erfüllen.[543] Die Rechtsunsicherheit bzgl. der Peer-to-Peer Handelsplattformen ist momentan aber noch gross. Im Herbst 2020 (aktualisiert im Herbst 2021) hat die Swiss Blockchain Federation immerhin einen Leitfaden für Unternehmen entwickelt, die an alternativen Handelsplattformen interessiert sind.[544]

Die Eigenart der verschiedenen Kategorien von DLT-Handelsplattformen ist bei der Entwicklung von möglichen Streitbeilegungsverfahren zu berücksichtigen. In diesem Sinne werden nachfolgend die zuvor erläuterten Dispute-Re-

539 Vgl. für ähnliche Regelungen im Ausland Kap. VI.A.2.

540 Ähnliche Grundsätze werden in den OECD Guidelines for Multinational Enterprises, 2011 Edition, Paris 2011, Part II, 67 ff. festgehalten; vgl. zum Ganzen *Weber*, 2018b, 101–117.

541 *Bundesrat*, 2018, 105 f.; vgl. im Detail auch Kap. III.D.2.

542 Zur Definition der zentralen und dezentralen Handelsplattformen vgl. *Bundesrat*, 2018, 146 f.

543 Vgl. auch Kap. III.D.1 und III.D.2.a).

544 SBF, 2021b, 9 ff.

solution-Verfahren auf ihre Tauglichkeit für die verschiedenen Handelsplattformen hin überprüft.

a) Gemeinsamer Ausgestaltungsansatz

Gewisse Grundsätze sind trotz der Eigenarten der verschiedenen Kategorien von DLT-Handelsplattformen sachlich zu regeln. Gemäss den Empfehlungen in den UNCITRAL Technical Notes und auch der Ausgestaltung der Dispute Resolution in Finanzmärkten ausserhalb der Schweiz ist die Entwicklung eines mehrstufigen Verfahrens angezeigt. Mithin ist denkbar, analog zur Regelung in Art. 74 ff. FIDLEG ein Vermittlungsverfahren vor einer Ombudsstelle einzuführen. Die Handelsplattformen wären dabei verpflichtet, sich einer Ombudsstelle anzuschliessen (analog Art. 77 ff. FIDLEG), welche der amtlichen Anerkennung bedarf (analog Art. 84 FIDLEG). Um das Verfahren den Teilnehmerinnen und Teilnehmern zugänglicher zu machen, ist ein kostenloses (oder ein mindestens für die Teilnehmerinnen und Teilnehmer kostengünstiges) Verfahren ratsam.

Darüber hinaus ist die Errichtung eines Mediations- und Schiedsverfahrens sinnvoll. Ab einer gewissen Höhe des Streitwerts (d.h. der grösseren Bedeutung des Verfahrens) soll es den Teilnehmerinnen und Teilnehmern freistehen, das Ombuds- bzw. Mediationsverfahren zu übergehen und unverzüglich in das Schiedsverfahren einzusteigen. Für die Schiedsverfahren können alle Teilnehmerinnen und Teilnehmer verpflichtet werden, bei jedem Vertragsabschluss auf einer DLT-Handelsplattform die Musterklauseln in die (individuelle) Verträge aufzunehmen.[545]

Ausserdem lässt sich für die Crowdsourced Arbitration[546] – unabhängig von der Kategorie der DLT-Handelsplattform – festhalten, dass deren Einrichtung

---

545 Für die Problematik der Aufnahme von Musterschiedsklauseln in die Smart Contracts vgl. *Guillaume/Riva*, 2022, 43, wonach eine Schiedsklausel im Smart Contract nicht die erforderlichen formellen Voraussetzungen erfüllen würde.

546 Die Crowdsourced Arbitration gleicht in ihren Grundzügen der On-Chain Arbitration; der eigentliche Unterschied liegt in der Entscheidfindung, welche gestützt auf eine unbestimmte und unbegrenzte Anzahl von «Gerichtsmitgliedern» stattfindet (*Fischer/Schneuwly*, 2021, 101 m.w.H.). Dabei stellt sich die Frage, *wer* bei der Entscheidfindung mitwirken sollte. Hierzu gibt es verschiedenste Möglichkeiten, welche von «nur eine spezifisch bestimmte Anzahl Leute» bis zu «alle Mitglieder der Plattform» reichen (WEF, 2020, 12 ff.). Im DLT-Bereich besteht zudem die Möglichkeit, ein Strafsystem für «falsche» Entscheidungen einzuführen (*Schmitz/Rule*, 2019, 118). Zur allgemeinen Möglichkeit dieser «dezentralen» Gerichtsbarkeit vgl. Ast/*Deffains*, 2021, 245 ff.

zum gegenwärtigen Zeitpunkt wohl noch nicht als realisierbar erscheint. Obwohl die Crowdsourced Arbitration der Grundidee der Anonymität auf der Blockchain am ausgeprägtesten Rechnung trägt, lässt sich die Einhaltung der allgemeinen Verfahrensgrundsätze (noch) nicht gewährleisten. Einerseits ist es fraglich, inwieweit unbekannte Laien geeignet sind, über komplexe Sachverhalt zu richten, andererseits weist das Bezahlungssystem[547] gewisse Tücken auf. Bei Kleros bezahlen die «Schiedsrichterinnen und Schiedsrichter» ihre Kaution mit dem Pinakion-Token (eine auf Ethereum basierende Kryptowährung von Kleros). Hält jedoch eine Person mindestens 51% dieser Token (bspw. über verschiedene Wallets), kann sie im Grunde genommen alleine über alle Entscheide bei der Crowdsourced Arbitration urteilen.[548] Ferner ist zweifelhaft, ob das Erfordernis der unparteiischen und unabhängigen Schiedsrichterinnen und Schiedsrichter eingehalten wird.

Zudem ist fraglich, ob der für die Crowdsourced Arbitration (voraussichtlich) charakteristische Ansatz der Game Theory überhaupt für die Streitbeilegung tauglich ist (beispielsweise die Plattform Kleros basiert auf der Game Theory). Bei der Game Theory handelt es sich um eine mathematische Theorie, die Entscheidungssituationen modelliert; die Plattform Kleros hat dieses Modell folgendermassen umgesetzt: Kleros verpflichtet die «Schiedsrichterinnen und Schiedsrichter» bei der Auswahl ins «Gericht», eine Kaution (grundsätzlich in Kryptowährung) zu hinterlegen. Wer die Entscheidung mit der Mehrheit des «Schiedsgerichts» fällt, bekommt zusätzlich zur eigenen Kaution auch noch die Kaution der Minderheit; «falsche» Entscheidungen werden also bestraft. Alle «Schiedsrichterinnen und Schiedsrichter» erhalten zudem eine Schiedsgebühr.[549]

547 Die Plattform Kleros verspricht eine schnelle, kostengünstige, vertrauenswürdige, transparente und dezentralisierte Streitbeilegungsmethode, welche auf der Game Theory aufbaut (*Palombo/Battaglini/Cantisani*, 2021, 130; *Allen/Lane/Poblet*, 2019, 93; *Schmitz/Rule*, 2019, 118; *Rabinovich-Einy/Katsch*, 2019, 59 f.).

548 *Schmitz/Rule*, 2019, 118 f.

549 *Palombo/Battaglini/Cantisani*, 2021, 130; *Allen/Lane/Poblet*, 2019, 93; *Schmitz/Rule*, 2019, 118; *Rabinovich-Einy/Katsch*, 2019, 59 f.

b) Zentrale Handelsplattformen

Auf zentralen Handelsplattformen treffen sich alle Teilnehmenden an einem Punkt und sind mit dem zentralen Netzwerk verbunden. Zudem sind sie auf die Mitwirkung der Handelsplattform angewiesen, da sie keinen direkten Zugriff auf die Transaktionsabwicklung haben; die faktische Verfügungsmacht über die DLT-Effekten liegt bei der Handelsplattform.[550]

Anders als bei der Consumer Dispute Resolution in der EU ist auf zentralen Handelsplattformen nicht zwingend eine ODR-Plattform erforderlich. Hingegen ist z.B. eine unabhängige Beschwerdeinstanz analog zu Art. 37 FinfraG einzurichten. Anstelle einer anschliessenden Klage beim Zivilgericht ist ein Verfahren über die On-Chain Arbitration empfehlenswert, um die Besonderheiten der DLT berücksichtigen zu können.

Die Idee, dass die Betreiberin der Blockchain, bzw. vorliegend der (zentralen) Handelsplattform, die Streitbeilegungsabrede in den Smart Contract implementiert, ist nicht neu;[551] indessen sind auch die Besonderheiten der Handelsplattformen zu beachten. Trotz bereits existierender Ideen bzgl. Implementierung der Streitbeilegungsabrede in den Smart Contract ist es gegenwärtig weiterhin empfehlenswert, in einem ersten Schritt die Schiedsklauseln in den Nutzungsvertrag der Handelsplattform aufzunehmen und so potenziellen (formellen) Ungewissheiten der Schiedsabrede im Smart Contract selbst entgegenzuwirken.

Um der Blockierung des Smart Contract zuvorzukommen und einen Dissens bei der Stellung eines Schiedsrichters bzw. Schiedsgerichts zu vermeiden, ist für Verfahren der On-Chain Arbitration die Bestimmung einer Ernennungsinstanz (engl. appointing authority) auf der Blockchain erforderlich.[552] Sobald eine Partei die Appointing Authority anruft, könnte diese automatisch das Schiedsverfahren einleiten.

Auf zentralen Handelsplattformen sind beide Varianten zur Unterbrechung des Smart Contract und zur Einleitung des Schiedsverfahrens anwendbar; beim Ansatz der Multi-Signature-Adressen kann die Betreiberin der zentralen Handelsplattform als Drittperson fungieren. Die Ausführung der Transaktion findet erst statt, nachdem die Betreiberin der Handelsplattform von der Be-

550 Vgl. Kap. III.D.2.b) m.w.H.

551 Vgl. *Kaal/Calcaterra*, 2017, 136; *O'Shields*, 2017, 191; *Koula*, 2016, 40–69.

552 Ähnliche (rudimentäre) Vorgehensweisen in diese Richtung existieren bereits, vgl. *Ortolani*, 2021, 217 f.

schwerdeinstanz (z.B. dem Schiedsgericht) den endgültigen Entscheid erhält. Auch denkbar ist, dass die Betreiberin – nach Erhalt des Entscheids – mit der kontrollierten Ausführung einer Fork die strittige Transaktion ändert oder rückgängig macht. Soll der Einbezug der Handelsplattform vermieden werden (z.B. für Streitigkeiten zwischen Plattform und Teilnehmenden), steht weiterhin die Möglichkeit des Zugangs zur Smart Contract Dispute Resolution Library offen.

c) Dezentrale Handelsplattformen

Auf dezentralen Handelsplattformen gibt es kein zentrales Netzwerk. Die Teilnehmenden können die DLT-Effekten ohne Mitwirkung der Handelsplattform auf Dritte übertragen. Die dezentrale Handelsplattform dient nur als Vermittlerin zwischen den Parteien und hat keine Verfügungsmacht über die DLT-Effekten. Die Parteien treffen sich lediglich auf der Handelsplattform.[553]

Ähnlich wie bei der Consumer Dispute Resolution in der EU kann bei dezentralen Handelsplattformen eine ODR-Plattform als Anlaufstelle dienen. Einerseits erlaubt die Plattform einen Überblick über die potenziellen Verfahrensschritte und andererseits fördert sie die leichte Zugänglichkeit des Verfahrens für die Parteien. Weil eine dezentrale Handelsplattform bloss als Vermittlerin zwischen den Parteien agiert, ist die Betreiberin der Handelsplattform nicht verpflichtet, (eigene) Beschwerdeinstanzen zu errichten. Es genügt, wenn die Teilnehmenden durch die ODR-Plattform auf verfügbare Verfahrensschritte aufmerksam gemacht werden.

Wie bei den zentralen Handelsplattformen ist auch für die dezentralen Handelsplattformen ein mehrstufiges Verfahren mit der Möglichkeit zur abschliessenden On-Chain Arbitration und einer Ernennungsinstanz empfehlenswert. Da jedoch die Teilnehmenden die DLT-Effekten ohne Mitwirkung der Handelsplattform auf Dritte übertragen können und die Plattform keine Verfügungsmacht über die Effekten hat, ist fraglich, ob tatsächlich autorisierte Teilnehmende existieren, welche ein Forking durchführen und so die strittige Transaktion ändern oder rückgängig machen könnten. Aus diesem Grund ist für die Unterbrechung des Smart Contract und die Einleitung des Schiedsverfahrens der Ansatz über die Smart Contract Dispute Resolution Library zu empfehlen.

553 Vgl. Kap. III.D.2.b).

d) Peer-to-Peer Handelsplattformen

Die Peer-to-Peer Handelsplattformen (bzw. distributed Handelsplattformen) weisen ebenfalls kein zentrales Netzwerk auf. Die Teilnehmenden übertragen keine Rechte an die Handelsplattform, sondern sie behalten die vollständige Kontrolle und Verfügungsmacht über ihre Daten im Rahmen der bilateralen Transaktionen. Eine Art von Handelsplattform kann in diesen Systemen jedoch vorgelagert sein, z.B. in Form von Bulletin Boards.[554]

Zur Ausgestaltung der Peer-to-Peer Handelsplattformen ist (noch) nicht viel bekannt;[555] trotzdem wird – deckungsgleich mit den dezentralen Handelsplattformen – auch auf den Peer-to-Peer Handelsplattformen eine zentrale Anlaufstelle bspw. in Form einer ODR-Plattform für eine leichte Zugänglichkeit des Verfahrens erforderlich sein. Da die Peer-to-Peer Handelsplattformen die Grundgedanken der Distributed Ledger-Technologie (u.a. Anonymität, distributed) am ausgeprägtesten aufweisen, erscheint die Entwicklung einer On-Chain Arbitration unerlässlich.

Da die Teilnehmenden auf Peer-to-Peer Handelsplattformen die Transaktionen untereinander ausführen, eignet sich zur Unterbrechung des Smart Contract und zur Einleitung des Schiedsverfahrens der Ansatz über die Smart Contract Dispute Resolution Library; dieses Vorgehen vermeidet den Beizug einer Drittperson, wie dies bei Multi-Signature-Adressen der Fall ist.[556]

Aufgrund ihrer Ausprägung als distributed Handelsplattform ist die Anwendung der Crowdsourced Arbitration am ehesten bei den Peer-to-Peer Handelsplattformen denkbar; jedoch sind auch insoweit noch einige Nachteile zu überwinden und potenzielle Lösungsansätze vertieft zu testen.

---

554 Vgl. Kap. III.D.2.b).

555 Immerhin hat die Swiss Blockchain Federation eine Unterscheidung zwischen dezentralen und Peer-to-Peer Handelsplattformen vorgenommen. Auf Peer-to-Peer Handelsplattformen erfolgt die Transaktion direkt zwischen den Teilnehmenden, während auf dezentralen Handelsplattformen die Teilnehmenden die Handelspartnerinnen und Handelspartner nicht selbst auswählen können, sondern automatisch mit dem besten Angebot zusammengeführt werden (vgl. SBF, 2021b, 9).

556 Ähnlich wie bei dezentralen Handelsplattformen ist auch hier fraglich, ob autorisierte Teilnehmende existieren, die ein Forking durchführen und so die strittige Transaktion ändern oder rückgängig machen könnten.

3. Konkretisierung der verfahrensbezogenen Regelungspunkte für DLT-Handelsplattformen

Angesichts der automatischen Ausführung der Smart Contracts und der unterschiedlichen Strukturen der jeweiligen Kategorien von DLT-Handelsplattformen eignet sich das «traditionelle» Rechtsverfahren nur bedingt für entsprechende Rechtsstreitigkeiten. Die Besonderheiten in diesem Sektor erfordern punktuelle Anpassungen der verfahrensbezogenen Regelungen; nachfolgend werden die relevantesten verfahrensrechtlichen Bestimmungen für die einzelnen Formen der DLT-Handelsplattformen angesprochen.[557]

a) Zentrale Handelsplattformen

Die Betreiberin einer zentralen Handelsplattform hat aufgrund ihrer Verfügungsmacht und der Kontrolle über die Transaktionsabwicklungen eine besondere Stellung mit gewissen Einflussmöglichkeiten inne. Die Teilnehmenden sind zwingend auf die Betreiberin der zentralen Handelsplattform angewiesen. Ausserdem erfolgt der Vertragsabschluss in einem zentralen System nach den von der Betreiberin festgelegten Regeln.[558] Dadurch bietet es sich auch in der Schweiz an, – ähnlich wie in Hong Kong, Singapur, den USA und China – die Streitigkeiten den staatlichen Gerichten zu entziehen und einem mehrstufigem Streitbeilegungsmechanismus mit Mediation und Schiedsgerichtsbarkeit zu unterwerfen.

Die Handelsplattformen können auf verschiedene Arten die Durchführung eines Mediation- bzw. Schiedsverfahrens erreichen. Einerseits lässt sich die Teilnahme auf zentralen Handelsplattformen beim Vertragsabschluss an die Unterzeichnung einer Schiedsvereinbarung mit vorgängiger Mediation knüpfen. Andererseits vermag eine Aktiengesellschaft mit tokenisierten Aktien die On-Chain Arbitration auch in ihren Statuten vorzusehen. Haben die Parteien die Streitigkeit den staatlichen Gerichten entzogen, können sie das Verfahren ihren Interessen entsprechend anpassen.

Die Mediation zielt auf eine Win-Win-Lösung mit einem kostengünstigen Verfahren ab; sie ermöglicht eine parteiautonome Lösung innerhalb beträchtlich kürzerer Zeit als vor staatlichen Gerichten.[559] Diese Vorteile erlauben gleichzeitig ein zugänglicheres Verfahren für die schwächeren Parteien. Aufgrund

---

557 Zu den Formen der DLT-Handelsplattformen, vgl. Kap. III.C.1.b), III.D.2.b) und V.A.3.

558 Vgl. Kap. V.A.3.b).

559 *Girsberger/Peter*, 2019, 470 ff.

der Mediationsklausel können sich die Parteien bei der vorgesehenen Mediationsstelle für ihre Streitigkeiten melden. Jedoch beruht das Mediationsverfahren auf der Eigenverantwortung und Freiwilligkeit der Parteien, d.h. jede Partei vermag die Mediation (auch nachträglich) abzulehnen. Ein Entscheid aus dem Mediationsverfahren ist für die Handelsplattform als bindend zu bewerten, während die Teilnehmenden diesen Entscheid vor das Schiedsgericht ziehen können sollten. Gelangen die Parteien im Rahmen der Mediationsverhandlung zu keinem befriedigenden Ergebnis, müssen sie das Recht haben, das Schiedsgericht anzurufen.

Liegt ein Verfahren von grossem Interesse für beide Parteien vor, lässt sich auch vorsehen, ohne Mediation sofort das Schiedsgericht anzurufen; dies ist bspw. bei Verfahren ab einer gewissen Höhe des Streitwerts denkbar. Anders als vor staatlichen Gerichten können die Parteien das Schiedsverfahren individuell gestalten; die Parteien sind bei der Schiedsgerichtsbarkeit regelmässig in der Lage, die Schiedsrichterinnen und Schiedsrichter selbst zu wählen. Dies ermöglicht den Parteien insbesondere bei komplexen Sachverhalten eine Wahl von Experten auf dem betreffenden Sachgebiet,[560] womit sich grundsätzlich die Qualität der Entscheide verbessert. Um ein solches Expertenwissen zu gewährleisten, braucht es sinnvollerweise ein institutionelles Schiedsgericht, welches eine Liste mit potenziellen Schiedsrichterinnen und Schiedsrichtern, die über Kenntnisse im Finanzdienstleistungssektor und im DLT-Bereich verfügen, zur Auswahl vorlegt;[561] es obliegt hernach den Parteien, jeweils ihre Schiedsrichterinnen und Schiedsrichter zu ernennen und so das Schiedsgericht zu bilden.

Schiedsverfahren erlauben grundsätzlich eine schnelle Lösungsfindung, da sie im Gegensatz zu staatlichen Gerichten bloss für die konkrete Streiterledigung zusammengesetzt werden und somit nicht überlastet sind.[562] Zwar ist auf zentralen Handelsplattformen eine On-Chain Arbitration denkbar, aber sie stellt nicht zwingend die beste Lösung dar. Aufgrund des zentralen Charakters und den damit zusammenhängenden Einflussmöglichkeiten des Systems ist den Anforderungen zur Durchführung eines Schiedsverfahrens bereits Rechnung getragen.

560 *Girsberger/Voser*, 2021, Rz. 134.

561 Als institutionelle Schiedsgerichtsinstanz mit Expertenwissen in diesem Bereich ist bspw. der Verein «ITDR – Institution for IT and Data Dispute Resolution» (http://www.itdr.ch), der mit der «Swiss Arbitration» (https://www.swissarbitration.org) seine ADR-Dienste im ICT-Sektor anbietet, zu erwähnen; vgl. auch Kap. VI.C.3.b).

562 *Kaufmann-Kohler/Rigozzi*, 2015, Rz. 1.44.

b) Dezentrale Handelsplattformen

Auf dezentralen Handelsplattformen hingegen sind die Teilnehmenden nicht zwingend auf deren Betreiberin angewiesen und können selbst auf die DLT-Effekten zugreifen. Die Betreiberin einer dezentralen Handelsplattform agiert bloss als Vermittlerin und hat keine Verfügungsmacht über die Vermögenswerte. Der Vertragsabschluss kommt – unter Zuhilfenahme eines Smart Contract – direkt zwischen Käuferin und Käufer sowie Verkäuferin und Verkäufer zustande, selbst wenn die technischen Regeln und Vorgaben der Handelsplattform gelten.[563] Da einerseits die Handelsplattform weiterhin die technischen Regeln und Vorgaben des Vertragsabschlusses bestimmt und andererseits der Vertrag zwischen den Parteien sich auf einen Smart Contract stützt, eignen sich dezentrale Handelsplattformen besonders für die Implementierung einer On-Chain Arbitration mit vorgängiger Mediation; die Einrichtung kann nach denselben Ansätzen wie bei zentralen Handelsplattformen erfolgen.

Die On-Chain Arbitration erlaubt eine angemessene Unterbrechung des Smart Contract und die Einleitung des Schiedsverfahrens auf verschiedene Arten. Bei Streitigkeiten zwischen den jeweiligen Teilnehmenden ist zu empfehlen, durch Multi-Signature-Adressen den Smart Contract anzuhalten; nach Erledigung des Schiedsverfahrens stellt die Plattform den erforderlichen, zweiten Schlüssel zur Verfügung, um die Ausführung des Smart Contract fortzusetzen. Liegt jedoch eine Streitigkeit zwischen den Teilnehmenden und der Plattform selbst vor, muss das Verfahren über die Smart Contract Dispute Resolution Library zur Anwendung kommen. Um die Durchführung des Schiedsverfahrens zu gewährleisten, ist eine Ernennungsinstanz zu bestimmen, welche bei Uneinigkeit der Parteien das Schiedsgericht bestellt. Bei der On-Chain Arbitration entfällt sodann potenziell auch die Problematik der Anerkennung und Vollstreckung des Schiedsentscheids, womit das Verfahren zusätzlich schneller zum Abschluss kommt.[564]

Die Streitigkeiten über die Smart Contracts können allenfalls bereits bestehenden institutionellen Schiedsgerichten unterworfen werden. Der Verein «ITDR – Institution for IT and Data Dispute Resolution»[565] bietet in Zusammenarbeit mit der «Swiss Arbitration» als neuer (fusionierter) Plattform seine ADR-Dienste im ICT-Sektor (inkl. Datenschutz) an.[566] Institutionelle Schieds-

563 Vgl. Kap. V.A.3.a) m.w.H.

564 Vgl. hierzu auch Kap. VI.B.2.d).

565 http://www.itdr.ch.

566 https://www.swissarbitration.org.

gerichte wie die «ITDR – Institution for IT and Data Dispute Resolution» sind im Bereich der DLT besonders erwünscht, weil die Streitfragen einen hohen Grad an Interdisziplinarität und grosses technisches und rechtliches Spezialwissen voraussetzen.

c) Peer-to-Peer Handelsplattformen

Aufgrund der Eigenschaften der verteilten Systeme erscheint es für Peer-to-Peer Handelsplattformen[567] als sinnvoll, eine ODR-Plattform einzurichten, welche den Teilnehmenden als zentrale Anlaufstelle für Streitigkeiten dient. Die ODR-Plattform kann einerseits eigene, rudimentäre Streitbeilegungsmechanismen anbieten und andererseits weitere zur Verfügung stehende Streitbeilegungsmechanismen aufzeigen und damit der einfachen Einreichung einer Beschwerde dienen. Analog zu Art. 74 ff. FIDLEG sollten die Peer-to-Peer Handelsplattformen verpflichtet sein, sich einer bewilligten Ombudsstelle anzuschliessen; dies erlaubt den Teilnehmenden eine einfache und kostengünstige Streitbeilegung. Die Errichtung der Ombudsstelle liegt sowohl im Interesse der Teilnehmenden als auch der Handelsplattformen selbst, da sie ein unbürokratisches, faires und unparteiisches Verfahren anbietet.[568]

Sind die Parteien mit der Entscheidung der Ombudsstelle nicht zufrieden, sollte die ODR-Plattform die Möglichkeit zur Eskalation des Verfahrens in Form der Mediation und der Schiedsgerichtsbarkeit anbieten. Die Ombudsstelle und das Mediationsverfahren sind dann hilfreich, wenn die Parteien daran interessiert sind, eine Lösung der strittigen Fragen zu finden; ansonsten bleibt bloss das Schiedsverfahren übrig. Die Implementierung der Mediations- und Schiedsklausel erfolgt nach denselben Ansätzen wie bei zentralen und dezentralen Handelsplattformen.

Da die Peer-to-Peer Handelsplattformen selbst keine Zentralisierung realisieren, ist die Aufnahme einer Schiedsklausel in vorgelagerte Verträge[569] (oder in den Statuten betroffener Aktiengesellschaften) unabdingbar. Andernfalls ergeben sich aufgrund der Ausgestaltung als distributed Handelsplattformen verschiedene Probleme, wenn ein ordentliches Gerichtsverfahren durchgeführt werden muss (Fragen zur Zuständigkeit, zum anwendbaren Recht, zur Voll-

567 Zu den Peer-to-Peer Handelsplattformen, vgl. Kap. III.D.2.b).

568 Vgl. Art. 75 Abs. 1 FIDLEG; vgl. ferner *Moser*, 2021, 76 f.

569 Denkbar ist auch die Implementierung der Schiedsklausel direkt in den Smart Contract. In diesem Fall ist aber noch nicht abschliessend geklärt, ob alle formellen Voraussetzungen tatsächlich erfüllt sind (vgl. hierzu Fn. 523, insb. kritisch *Guillaume/Riva*, 2022, 43).

streckbarkeit). Fraglich ist immerhin, inwiefern die Handelsplattform tatsächlich Einfluss auf die Ausgestaltung des Smart Contract hat und die Teilnehmenden verpflichten kann, eine Schiedsklausel in den Vertrag einzubauen, weil die Handelsplattform eine Art «vorgelagerte Handelsplattform» ohne Zentralisierung und Verfügungsmacht ihrer Betreiberin ist.[570] Ungeachtet dessen stellt auch für die Peer-to-Peer Handelsplattformen die On-Chain Arbitration mit dem bereits erwähnten Verfahrensablauf ein sinnvolles Streiterledigungsverfahren dar.

[570] Vgl. Kap. III.D.2.b).

VII. Ausblick

Mit dem neuen DLT-Gesetz hat der Gesetzgeber die rechtlichen Grundlagen für innovative Lösungen betreffend der DLT-Geschäftsmodelle gelegt. Dennoch bleibt abzuwarten, welchen Herausforderungen sich die Betreiber der DLT-Handelssysteme zu stellen haben und welche Anforderungen in der Praxis Probleme bereiten werden. Da die Schweiz eines der ersten Länder ist, das eine gesetzliche Regelung für die DLT-Handelssysteme in Kraft gesetzt hat, gibt es noch kaum Anwendungsbeispiele; aus diesem Grund wird sich die Effizienz und Funktionsfähigkeit des DLT-Gesetzes erst zeigen müssen.

Bereits vor Erlass des DLT-Gesetzes ist die Vermutung geäussert worden, dass aufgrund des gesetzlichen Rahmens mit den strengen Bewilligungsvoraussetzungen und den recht weitgehenden Überwachungskriterien die Zahl der von der FINMA künftig zu bewilligenden DLT-Handelsplattformen klein bleiben dürfte;[571] diese Vermutung scheint sich zwischenzeitlich zu bestätigen. Nur wirtschaftlich starke Unternehmen sind in der Lage, das dichte Regulierungswerk zu bewältigen bzw. dieses in der Realisierung des Geschäftsmodells hinzunehmen. Gleichzeitig dürfen die aufsichtsrechtlichen Anforderungen v.a. für (kleinere) Handelsplattformen nicht zu hoch sein (was aus heutiger Sicht als zweifelhaft erscheint[572]), um zu vermeiden, dass entsprechende Aktivitäten ins Ausland verlagert werden; insoweit besteht ein Interesse der Schweiz, ein liberales Regulierungsregime zu verwirklichen.

Im Rahmen der Sicherheit und Resilienz bei DLT-basierten Finanzmarktinfrastrukturen lässt sich auf den ersten Blick festhalten, dass der Gesetzgeber mit der (indirekten) gesetzlichen und regulatorischen Verpflichtung zur Verwendung von permissioned DLT-Handelsplattformen viele DLT-basierten Sicherheitsbedenken ausgeschlossen hat. Dadurch lässt sich das Hauptaugenmerk

---

571 Die SIX Digital Exchange (SDX) hat sich nicht für eine DLT-Handelssystem-Lizenz beworben, sondern eine vollständig regulierte, integrierte Handels-, Abwicklungs- und Verwahrungsinfrastruktur basierend auf der DLT als Börse und Zentralverwahrer durch die FINMA bewilligen lassen (FINMA, Medienmitteilung – FINMA bewilligt erstmals Börse und Zentralverwahrer für Handel mit Token vom 10. September 2021, aufrufbar unter <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/8news/medienmitteilungen/2021/09/20210910-mm-sdx.pdf?sc_lang=de&hash=4F2AF725EF87564355B5AA6815615D51>).

572 Dazu auch Kap. III.C.4 und insbesondere Kap. III.D.; vgl. auch SBF, 2021b, 9 ff.

fast ausschliesslich auf die Beseitigung der herkömmlichen Herausforderungen richten, die grundsätzlich mit derselben Herangehensweise zu bewältigen sind, wie dies im Bereich der Cybersicherheit und Cyber-Resilienz auf «traditionellen» Finanzmärkten der Fall ist. Das schliesst aber nicht aus, dass die DLT-spezifischen Gefahren weiterhin zu überwachen sind; da sich die DLT stetig weiterentwickelt, können neue Angriffsmöglichkeiten aufkommen oder auch neue Lücken im DLT-System selbst auftreten, die zurzeit noch unbekannt sind. Der Gesetzgeber hat die Möglichkeit, gestützt auf internationale Standards und Best Practices entweder Co-Regulierungen zu erlassen, um eine gewisse internationale Einheitlichkeit zu erreichen, oder in einer Sandbox eigene Ideen mit den Akteuren auf dem Schweizer Finanzplatz zu testen.

Bei der Beurteilung der schuldrechtlichen Transaktionsabwicklungen und der sich daraus ergebenden Haftungsaspekte ist massgeblich, ob die Vertragsbeziehungen zwischen den eigentlichen Transaktionsparteien (Verkäuferinnen und Verkäufer, Käuferinnen und Käufer) und den Anbieterinnen und Anbietern eines Wertrechteregisters oder einer DLT-Handelsplattform werkvertragliche oder auftragsrechtliche Elemente aufweisen; dementsprechend kommen für die jeweiligen Elemente die Regeln des Werkvertrags bzw. des Auftrags zur Anwendung. Die Erfolgselemente mit Bezug auf Transaktionsabwicklungen sprechen überwiegend für werkvertragliche Elemente. Dennoch kommen, wie die Erfahrungen mit dem Einsatz des Internet als Infrastruktur in den letzten 20 Jahren gezeigt haben, auf die Anbieterinnen und Anbieter keine unübersehbaren Haftungsrisiken zu. Spezialgesetzliche Haftungsordnungen müssten noch ausgearbeitet und in Kraft gesetzt werden. Wer das Register bzw. die Plattform sorgfältig «konstruiert» und betreibt, wird also erfolgreich im Markt der DLT-Geschäftsmodelle auftreten können.

Da die DLT-Vorlage keine gesetzlichen Regeln mit Bezug auf Streitbeilegungsmechanismen für DLT-Handelsplattformen vorsieht, besteht zwar Rechtsunsicherheit bzgl. der zukünftigen Ausgestaltung der Streitbeilegungsmethoden, aber dieser Umstand erlaubt gleichzeitig die Implementierung individueller Lösungsansätze für die verschiedenen Kategorien von DLT-Handelsplattformen. Zurzeit lässt sich kaum abschätzen, welche Typen der DLT-Handelsplattformen sich in der Praxis durchsetzen werden. Trotzdem ist angesichts der Entwicklungen in der DLT voraussehbar, dass die Verfahren der DLT-Handelsplattformen ein Mindestmass an Digitalisierung aufweisen. Da sich staatliche Verfahren nur bedingt für die DLT eignen, erweisen sich die verschiedenen Ausgestaltungsmöglichkeiten für ADR-Verfahren als zukunftsgerichtete Anknüpfungspunkte der DLT-Streiterledigung. Um im Gleichschritt mit den bestehenden Einrichtungen der Privatwirtschaft den zukünftigen, technologi-

schen Entwicklungen angemessen Rechnung zu tragen, erscheint es als unerlässlich, in absehbarer Zeit regulatorische Mindestanforderungen im Bereich der DLT-Handelsplattformen auszuarbeiten. Insoweit ist aber nicht zwingend der Gesetzgeber gefordert, sondern sinnvolle Standardisierungen lassen sich auch durch Arbeiten von Branchenverbänden erreichen.

Gesamthaft betrachtet lässt sich sagen, dass die Schweiz mit dem DLT-Gesetz angemessene gesetzliche Rahmenbedingungen geschaffen hat. Verschiedene spezifische Problembereiche bedürfen aber noch einer intensiveren Durchdringung und die Aufsichtsbehörden sollten in der Anwendungspraxis auch nicht immer restriktiver werden (z.B. im Kontext der Anforderungen an Handelsplattformen und an die Verwahrung). Auch die Nachfrage nach Angeboten im Bereich von DLT-Handelstransaktionen hält sich bisher in überschaubarem Rahmen.[573] Weitere (politische) Anstrengungen bleiben also notwendig, um die Standortqualität der Schweiz international und mit Bezug auf grenzüberschreitende Wertschöpfungsketten gut zu positionieren.

573 *Weber/Kuhn*, 2021a, Rz. 9.

Veröffentlichungen des Center für Information Technology, Society and Law (ITSL) der Universität Zürich

erschienen bei Schulthess Juristische Medien AG, Zürich

Vol. 1: **Werbung – Online**
FLORENT THOUVENIN/ROLF H. WEBER (Hrsg.)
Zürich 2017

Vol. 2: **Transatlantic Data Protection in Practice**
ROLF H. WEBER/DOMINIC N. STAIGER
Zürich 2017

Vol. 3: **Endorsements and Behavioral Advertising in Social Media under EU, Swiss, and US Law**
MANE SARGSYAN
Zürich 2017

Vol. 4: **Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte/ Utilisation des services de cloud par les avocates et avocats**
CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER
Zürich 2019

Vol. 5: **Die Informationspflichten des Unternehmers im E-Commerce**
DOMINIC OERTLY
Zürich 2019

Vol. 6: **Der IT-Outsourcingvertrag im schweizerischen Recht**
ALEXANDER SCHMID
Zürich 2019

Vol. 7: **Elemente einer Datenpolitik**
FLORENT THOUVENIN/ROLF H. WEBER/ALFRED FRÜH
Zürich 2019

Vol. 8: **Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht**
DAMIAN GEORGE
Zürich 2021

erschienen bei EIZ Publishing, Zürich

Vol. 9: **Cybersicherheit und Cyber-Resilienz in den Finanzmärkten**
ROLF H. WEBER/OKAN YILDIZ
Zürich 2022

Mit dem DLT-Gesetz verfügt die Schweiz über einen flexiblen Rechtsrahmen für innovative digitale Geschäftsmodelle. Die neu geschaffenen DLT-Handelsplattformen erleichtern grundsätzlich die Transaktionen mit tokenisierten Kryptowerten. In der Praxis stellen sich indessen noch viele praktische und rechtliche Herausforderungen. Nicht nur sind die gesetzlichen Vorgaben relativ einschränkend, sondern Resilienz und Systemstabilität verdienen auch grosse Aufmerksamkeit. Zudem sind Formen der alternativen Streitschlichtung zu finden. Das Buch erläutert das regulatorische Umfeld der DLT-Handelsplattformen und entwickelt praxisnahe Lösungen für die sich stellenden rechtlichen Probleme.